June 2011
Issue 15

Magazine NetworkSet

First Arabic Magazine for Networks

ماهو الفرق بين شهادتي
CCSP Vs CCNP

تعرف على بروتوكول
CDP

الشبكات في عالم ابل

المعايير الخاصة بطبقة
DATA LINK LAYER

الموجه Router
& التوجيه Routing

أجهزة البلوتوث وعلاقتها بعالم الشبكات



شهادة شكر وتقدير
للمهندس فادي الطه

الأمل

كثيرة هي الأفكار التى تراودني وكثيرة هي الأشياء التى تدفعني لأن أضع بصمتي, وكثيرة هي الدوافع التى تجبرني أن أغير الواقع العربي, وكثيرة هي الأحلام التى أأمل أن تتحقق في يوما من الأيام, لكن أكثر من كل هذا الأشياء أجد الأحباطات والأبواب المغلقة في وجهي دائما, لكن الأمل والشعور بأن الله معي وبأن أرادة الأنسان لا أحد يستطيع أيقافه هي دوافعي للمواصلة في الطريق الذي أخترته والذي دفعني لأضحي بأشياء عزيزة كانت على نفسي لكن أحمد الله وأقول حسبي الله ونعم الوكيل.

دققت الأبواب ووجهت الرسائل وطلبت المقابلات وأرسلت مئات الدعوات لكل من يستفيد من كل ما أفعله لصالح أمتي العربية المسلمة لكن كلها كانت بلا جدوى ولكن هيهات أن يكسر عزيمتي باب يغلق أو شخص أطلب مقابلته من أجل عرض مشاريع للمحتوى العربي على الأنترنت ويقولوا لي بأنه مشغول وبأنه سوف يتصلوا بك لاحقا.(يا لا سخافتكم وسذاجتكم)

إلى متى يا أمة العرب ترسلوا هذه المليارات نحو بناء ناطحات السحاب وأعاجيب الأرض و ترفضوا مشاريع ترتقي بها أمتنا بحجة أن لا عائد لكم من هذه المشاريع!!!. كيف بالله عليكم ؟ إلى متى يا أمة العرب نجلس ننتظر من الغربي أن يأتي ويعلمنا كيف نتعامل مع تقنياتهم العلمية ؟ إلى متى يا أمة العرب نصرف من خيرات ما أعطانا الله نحو مشاريع فاشلة وأن كانت ناجحة في البداية فهي فاشلة في النهاية ؟

لن أطرح المزيد من التساؤلات فهي لن تنتهي ولن يستطيع أحد الرد عليها فالكل جالس الآن يقرأ ويشعر بالحقيقة المرة ولكن شعوره ينتهي مع أنتهاء هذا المقال, فلقد مللت من كل واحد قرأ وأحس وصمت ولم يحرك ساكنا فأن تقول أنا معكم وأنا مستعد للعمل هو شيئ تافه وقد ألفته كثيرا ولم أعد أصغي إليه لأن الشخص الذي يريد أن يبدأ لن ينتظر الأشارة ولن ينتظر رد يقول له أهلا وسهلا بك معنا بل يبادر مباشرة وبعدها يقول أنا أصبحت معكم.

هذه المقالة لن أوجهها لأحد من القراء المستهلكين بل سوف أوجهها لنفسي ولكل شخص ساندني وبادر معي واقول لاتيأس أبدا فكل باب يغلق يفتح في مقابله ألف باب فطالما الله موجود فأن الأمل سوف يبقى موجود إلى الأبد وأن تسقط مرة في حياتك فهو من أجل أن تتعلم أن السقوط وجد من أجل أن تتعلم كيف تقف من جديد وبشكل أقوى وبعزيمة أكبر إن شاء الله فبالرغم من كل الأنتكاسات التى واجهتها والخسارات التى حصدتها نتيجة أستهتاري ببعض الأمور أجد أن الأمل هو ماتبقى لي وهذا الامل هو أن أرى غد عربي أكثر إشراقا من قبله وبأن أرى أشخاص يشاركوني العمل ويساندوني, لذلك سوف تجدوا مني مشروع جديد كل فترة وكلما سمحت الفرصة ومشروعي الجديد قادم أن شاء الله والذي أطلقت عليه ثورة تقنيات المعلومات أقتباسا من ربيع الثورات العربية وأعدكم بأن لا أتوقف أبدا طالما الوقت والزمن يسمح لي بهذا فالآن لم يعد لدي شيئ لكي آخسره إلا أن أخسر دعواتكم لي ودمتم بود.

أيمن النعيمي - سوريا



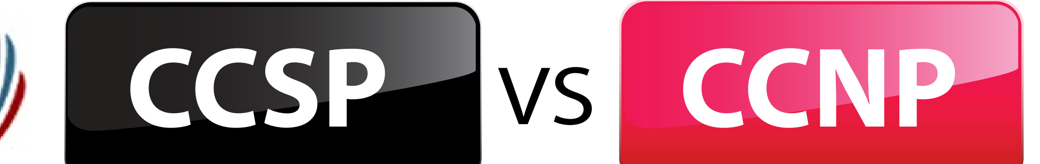
Magazine
NetworkSet
First Arabic Magazine for Networks

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

www.networkset.net

تقرؤون في هذا العدد





Security

شريف مجدي - مصر

: (CCSP) cisco certified security professional

معظمنا يعرف هذه الشهاده ولمن لا يعرفها فهي شهادة تقدمها Cisco في مجال ال Security اي انها تؤهل الحاصل عليها على التعامل مع حلول Cisco التى تقدمها في هذا المجال اما عن طريق الـ feature او اضافة معينه او جهاز كامل مخصص لاغراض الامن و الحمايه , بالاضافه الى منحك معرفة ودراية جيدة بالهجمات الموجه للشبكة و كيفية التصدى لها _عن طريق اجهزتها طبعا_ ارجوا ملاحظة اننى قلت «معرفه» و ليس «تجربة او تطبيق» فكلمة Security بمجرد ان تدخل فى اسم شهاده ما تجد الدارسين يتهافتون للدراستها لاكتساب مهارات ال Hacking او الاختراق , و لمن ينوى دراسه CCSP _او حتى CCNP SEC_ لهذا الغرض فالافضل ان يفكر قبل ان يبدأ و يحاول مع شهاده اخرى مثل CEH على سبيل المثال اذا كان هدفه تطبيق الهجوم بصورة عمليه , اما فى CCSP فما ستجده مختلف تماما , فقد يعطيك شرح للهجوم و لكن بطريقة نظرية والهدف من ذلك هو تمكينك من فهم الطريقة التى سيقدمها لك لحماية الشبكة من هذا الهجوم .

هناك ايضا جزء مهم جدا و هو يشكل نسبة كبيرة من المنهج وهو بخصوص شىء يدعى Policy Enforcing ما معنى هذا المصطلح ؟

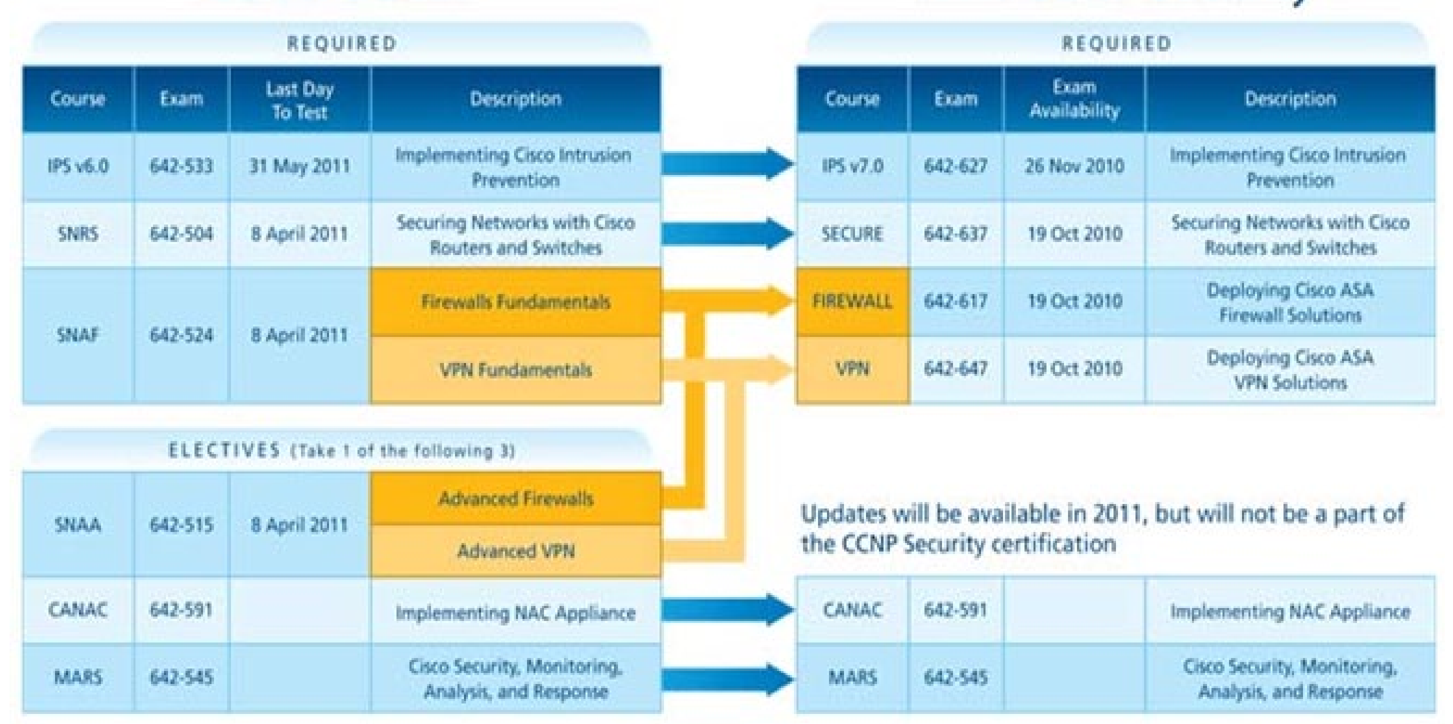
عندما تقوم شركة ما ببناء شبكة لها فاول شىء يجب تحديده هو الهدف من بناء هذه الشبكه , حسنا و هذا يلزم كتابة سياسة Policy لتنظيم العمل على الشبكه فعلى سبيل المثال عندنا شبكه بها server معين يقوم بتشغيل Application يدعى X وهذا كل ما نريده من هذه الشبكة ويستطيع المستخدمين ان يقوموا بعمل Access لهذا السيرفر فقط لا غير , لذلك فلا يجب السماح لاى traffic ان يمر فى الشبكه غير الذى حددناه فى ال Policy ولان مستخدمي الشبكه ليسوا بملائكة فيجب تحويل هذه ال Policy او السياسة المكتوبة او الموجوده على ورق الى اوامر حقيقية على اجهزة الشبكة من روترات و سويتشات و جدران نارية و اجهزة منع التطفل الى اخره ... اى اننا قمنا بتنفيذ سياستنا بالقوة و عدم الاعتماد على التزام المستخدمين للتعليمات التى حددتها ال Policy , و هذا يعطى control او تحكم كبير بالشبكة , و اروع ما تقدمه cisco فى هذا المجال هو مقدره اجهزتها على مراقبه كل صغيرة و كبيرة تحدث فى الشبكة و منعه او السماح له و ذلك حسب قرار مدير الشبكه .

باختصار من يحصل على هذه الشهاده _عن طريق المذاكرة الحقيقية طبعا_ يمكن ان نطلق عليه هذا التعريف «هو شخص محترف فى تطبيق حلول cisco الامنيه و ادراة اجهزة الامن و الحمايه التى تطرحها و التعامل مع البروتوكولات الخاصة في هذه الامور» .

اخيرا احب ان اقول معلومة بسيطة هو انه لم يعد هناك شىء يسمى CCSP حيث تم الغاء جميع امتحاناتها , فاثناء قراءتك لهذه السطور فاعلم ان اخر ميعاد لحجز اى امتحان من امتحاناتها قد انتهى . و حلت محل هذه الشهاده شهاده جديده تسمى CCNP Sec فلنتعرف على الشهادة الجديدة .

: CCNP Security

هي شهادة جديدة من cisco حلت محل الشهاده القديمة CCSP و نفس الكلام الذى قرأته فى الفقرة السابقة عن شهاده CCSP ينطبق تماما على CCNP Sec اذن ما الفرق ؟ الفرق اغلبه فى تقسيم المواد لكل شهاده و بالتالى تغير الامتحانات و محتوى كل امتحان و النقاط التى سيختبرك بها . هذا بالاضافه الى بعض المواضيع الجديده التى تم ادخالها على CCNP sec و التى كان من الممكن عمل تعديل بسيط على ال Exam Objective و لكن cisco ارادت اعاده هيكله شهاده CCSP بكاملها لتخرج بشكل جديد تماما لتناسب ال Job Role لـ security engineer كما تقول Cisco . اكملوا معى حتى نتعرف على نقاط الاختلاف بين المواد فى كل شهاده



Current CCSP

REQUIRED

Course	Exam	Last Day To Test	Description
IPS v6.0	642-533	31 May 2011	Implementing Cisco Intrusion Prevention
SNRS	642-504	8 April 2011	Securing Networks with Cisco Routers and Switches
SNAF	642-524	8 April 2011	Firewalls Fundamentals
			VPN Fundamentals

ELECTIVES (Take 1 of the following 3)

Course	Exam	Last Day To Test	Description
SNAA	642-515	8 April 2011	Advanced Firewalls
			Advanced VPN
CANAC	642-591		Implementing NAC Appliance
MARS	642-545		Cisco Security, Monitoring, Analysis, and Response

New CCNP Security

REQUIRED

Course	Exam	Exam Availability	Description
IPS v7.0	642-627	26 Nov 2010	Implementing Cisco Intrusion Prevention
SECURE	642-637	19 Oct 2010	Securing Networks with Cisco Routers and Switches
FIREWALL	642-617	19 Oct 2010	Deploying Cisco ASA Firewall Solutions
VPN	642-647	19 Oct 2010	Deploying Cisco ASA VPN Solutions

Updates will be available in 2011, but will not be a part of the CCNP Security certification

Course	Exam	Exam Availability	Description
CANAC	642-591		Implementing NAC Appliance
MARS	642-545		Cisco Security, Monitoring, Analysis, and Response

سأستعين بالصورة السابقة حتى استطيع توضيح الفرق بين مواد كل من CCSP & CCNP Sec . واضح فى الصورة ان شهاده CCSP تلزم اجتياز اربع امتحانات فقط , اول ثلاث امتحانات Required اى اجباري ولا يوجد حل اخر سوى اجتيازهم , بعد ذلك يتبقى امتحان واحد تختار بين عده امتحانات وذلك حسب اختيارك ويسمى هذا الامتحان Elective اى اختياري , دعونا نتحدث عن المواد الثلاثة الاولى الاجبارية بشكل مفصل و الماده الاختيارية :

المادة الاولى: SNRS - securing network with cisco routers and switch

بالنسبه لهذه الماده فهى تخوض فى تطبيق حلول cisco الامنية وتطبيقها على روترات وسويتشات cisco و خط تحت «روترات و سويتشات» فهذا معناه انك لن تستعين باى جهاز اخر ليوفر لك امن و حمايه الشبكه سواء كان IPS- IDS -ASA- PIX- NAC Appliance اي ان كل الاعتماد على الروترات و السويتشات و الخدمات التى تقدمها فى مجال ال security , و من امثلة المواضيع التى ستجدها هي كيف تقوم بتشغيل الروتر كجدار نارى FIREWALL او جهاز منع التطفل IPS وايضا تطبيق ال VPN بكل انواعها المختلفه سواء كانت IPsec او SSL وهذا على الروترات فقط , و ايضا بعض خصائص ال security الموجوده على الروترات والسويتشات .

الماده الثانيه implementing IPS - ٦.IPS v

هذه هى ثاني مواد CCSP الاجبارية حيث تمنحك بعض الخبرة فى التعامل مع اجهزة منع و كشف التطفل IPS & IDS و معرفة آلية عمل هذه الاجهزة , تعتبر من اسهل المواد في الشهاده لبساطتها و خلوها من التعقيد .



المادة الثالث SNAF - securing network with ASA FOUNDATION

ثالث مواد الشهادة و تبدأ معك فى جهاز جديد لم تتعامل معه من قبل و هو ASA , هذا الجهاز العبقري الذي يقوم بالعديد من المهام , بعض الناس تطلق عليه كلمه Firewall , ولكن فى الحقيقة مهام ال Firewall-ing قد لا تمثل سوى ثلث ما يقوم به هذا الجهاز , لاقرب لك فكرة يمكنني ان اقول انه عبارة عن ثلاثه اجهزة مختلفه فى جهاز واحد وهم PIX firewall & IPS sensor &VPN concentrator in ONE-BOX .
اعتقد ان الجمله السابقة تفى بالغرض وبالنسبه لل VPN concentrator فهو لمن لا يعرفه جهاز كانت تنتجه cisco _و اوقفت دعمه_ يقوم بمهام انهاء اتصالات ال VPN , نعود مرة اخرى الى ماده ال SNAF فهي ستوهلك للتعامل مع هذا الجهاز و لكن ستعلمك فقط ما هو اساسي او ضرورري فقط ولن تتعمق فى تفاصيل كثيرة , و لعلك لاحظت كلمه Foundation فى اسم الماده .

المادة الاختيارية SNAA OR CANAC OR MARS

عليك الان ان تختار ماده من الثلاثه و لدراستها حتى تحصل على الشهاده معظم الدراسين كانوا يختاروا ماده SNAA و سأتحدث عنها بالتفصيل بعد قليل , بالنسبه للمادتين الاخرتين فلا داعى الى التحدث عنهم حيث تم الغائهما نهائيا فى الشهاده القديمة و الجديدة ايضا فال CANAC تتحدث عن تطبيق NAC فى الشبكة و ال MARS هو جهاز تحليل و مراقبه لاى EVENT تحدث فى الشبكة .
السبب الذى كان يجعل معظم الدارسين يختارون ماده SNAA هو انها عبارة عن امتداد للماده السابقة SNAF فالاولى تعطى الاساسيات فقط و ال SNAA تتعمق فى تفاصيل اكبر حيث ان الاسم الكامل للماده هو Secure Network with ASA ADVANCED و الاسم يوضح كل شىء , ال SNAA تتشابه كثيرا مع ماده ال SNAF الفرق هو فى التفاصيل لذلك فلن تجد بها صعوبة تذكر لانك كنت على درايه بهذه المواضيع فى SNAF ستأخذ بعض التفاصيل فقط .

هكذا نكون انتهينا من CCSP فدعونا ننتقل الى CCNP SEC

بالنسبه ل CCNP SEC فجميع المواد بها اجبارية و لا يوجد عندك فرصة الاختيار مقارنة ب CCSP و الاربع مواده هي كالآتي :

المادة الاولى SECURE :

مجرد تغير مسمى لل SNRS فى CCSP نفس المواضيع التى تحدثنا عنها في CCSP ستعرفها وبعض الاضافات البسيطة جدا .

المادة الثانيه IPS v ٧ :

مجرد تحديث ل v.6 و به بعض الاضافات .

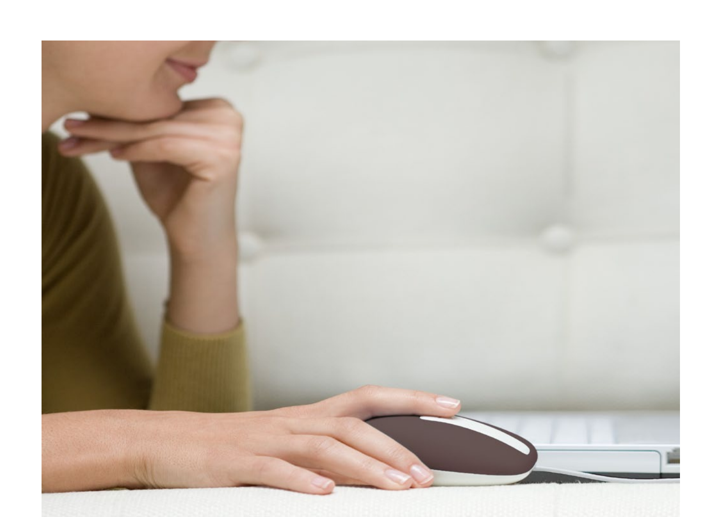
المادة الثالث Firewall :

هنا يبدأ الاختلاف بين الشهادتين , تتكلم هذه الماده عن ال ASA ولكن من ناحية واحده فقط و هى ك FIREWALL ليس اكثر ستعرف كل شىء عن ال ASA سواء كان Foundation OR Advanced ولكن ك firewall و ليس VPN concentrator حيث ان لل VPN ماده خاصه .

المادة الرابعه VPN :

ايضا تخوض فى تطبيقات ال VPN سواء كانت Foundation او Advanced على ال ASA

يمكننا ان نوضح الفرق بين اخر مادتين فى كل شهاده كالتالى :
CCSP - ASA advanced - ASA Foundation
CCNP Sec - Firwall (everything) - VPN ((everything
اتمنى ان اكون قد اجبت عن اى تساؤل حول الشهادتين , والى لقاء اخر فى مقالة جديدة .



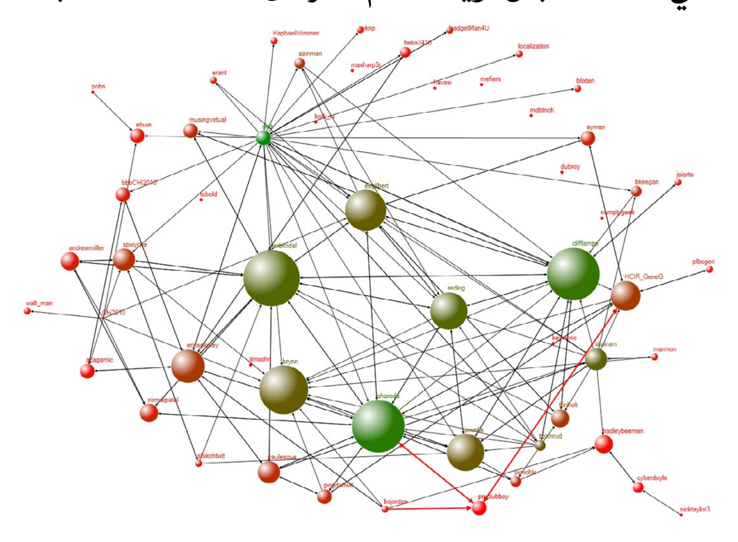
أوامر بروتوكول CDP :

أثناء دراستي لمنهج CCNA في اكاديمية سيسكو صادفتني إحدى الأدوات المستخدمة في حل مشاكل الشبكات، والتي خصصتْ لها سيسكو عدد من الصفحات بالرغم من بساطتها. لم أهتم لها في ذلك الوقت الى ان جاء اليوم الذي سألني فيه احد الأصدقاء عن طريقة لإستكشاف الشبكة بالرغم من اننا درسنا المنهج سويةً ولكن كما توقعت ووجدت فان الكثير من الذين أكملوا المنهج لا يتذكرون شيئاً عن هذه الأداة، وكذلك لم أجد موضوع معرب بشكل مفهوم يشرح عملها حيث ان اغلب (ان لم يكن جميع) ماوجدته عبارة عن نسخ ولصق من برامج الترجمة وهذه الاشياء التي جعلتني اكتب هذا المقال.

بداية ولأنني افضل الشرح الواقعي فلنفترض انك مهندس شبكات جديد في شركة ما و طُـلب منك صيانة او إعادة تنظيم الشبكة الخاصة بهذه المؤسسة وعرفت بأن المهندس الذي قبلك لم يترك أي وثائق تكفي لفهم هيكلية وتصميم الشبكة ماعدا معلومة صغيرة تخبرك بأن الباسوورد لجميع الراوترات هو (cisco)، لذلك مهمتك الاولى سوف تبدأ باعادة رسم الشبكة.. فما هو الحل إذن؟



الحل هو في استخدام البروتوكول (Cisco Discovery Protocol) الخاص بشركة سيسكو والمطور من قبلها. حيث يعتبر هذا البروتوكول من أبسط البروتوكولات في هذا المجال ويستخدم لغرض أستكشاف الشبكة



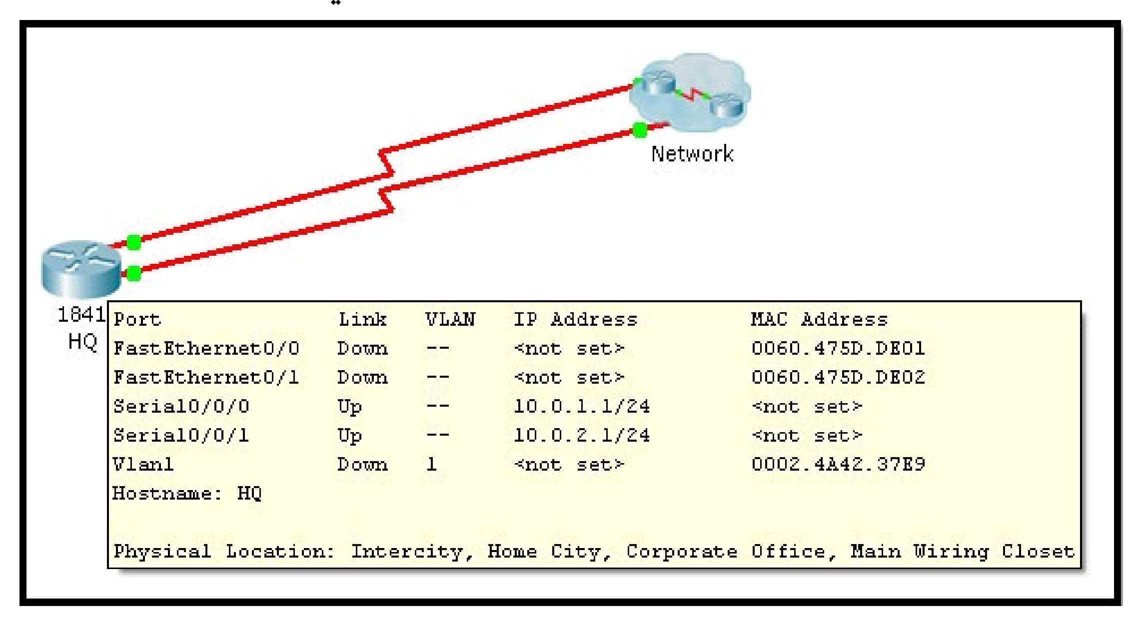
وتبادل المعلومات حول الأجهزة المرتبطة لغرض تصور الهيكلية التي تم بناء الشبكة وفقها، هذه المعلومات ترسل الى العنوان (0C-CC-CC-CC-00-01) وهو Multicast MAC Addressكل 60 ثانية عبر المنافذ التي تدعم تقنيات الايثرنت و ATM وFrame Relay ، بالاعتماد على قاعدة بيانات وهمية تسمى MIB وهي مختصر Management Information Base والتي يتم فيها تجميع المعلومات الخاصة بالشبكة لتستغل الاجهزة مصدر المعلومات هذا والذي يعتبر مركز المعلومات الخاص ببروتوكول الـ SNMP وللمزيد حول هذا الموضوع راجع الأعداد السابقة من المجلة.

سوف لن نتوسع في تفاصيل وآلية عمل هذا البروتوكول وخصائصه لكونه موضوع بحد ذاته ولكننا الان بصدد معرفة كيفية استعمال ادوات هذا البروتوكول والاستفادة من ميزاتها. ولذلك سوف نبدأ بالتعرف على اول واهم اداة وهو الامر

SHOW CDP NEIGHBORS DETAIL

ولفهم هذا الامر سنأخذ مثال عملي يوضح ذلك :

- لنفترض ان الشبكة الخاصة بالمؤسسة على النحو التالي :



حيث ان HQ هو الراوتر المركزي والذي عن طريقه سوف نتعرف على باقي اجزاء الشبكة المجهولة. فعند تنفيذ الامر SHOW CDP NEIGHBORS DETAIL سوف تكون النتيجة كالتالي :

```
HQ#show cdp neighbors detail

Device ID: RandD
Entry address(es):
  IP address : 10.0.2.2
Platform: cisco C2800, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/2/1
Holdtime: 123

Version :
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(14)T7, RELEAS
E SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Wed 3-Nov-06 06:50 by miwang

advertisement version: 2
Duplex: full
---------------------------

Device ID: Marketing
Entry address(es):
  IP address : 10.0.1.2
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0
Holdtime: 124

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full

HQ#
```

من المعلومات الناتجة يتبين لنا ان الراوتر HQمرتبط مع راوتر RANDD عن طريق المنفذ SERIAL 0/0/1 في الراوتر الحالي والمنفذ SERIAL 0/2/1 في الراوتر الآخر، أيضاً نستنتج ان الراوتر RANDD هو من نوع CISCO ومن فئة 2800. وكذلك الحال بالنسبة للراوتر MARKETING.

```
HQ>telnet 10.0.2.2
Trying 10.0.2.2 ...


User Access Verification

Password:
RandD>show cdp neighbors detail

Device ID: NewProducts
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/24
Holdtime: 146

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(
fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2
Duplex: full
---------------------------

Device ID: HQ
Entry address(es):
  IP address : 10.0.2.1
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/2/1, Port ID (outgoing port): Serial0/0/1
Holdtime: 146
```

كذلك من اهم المعلومات التي تظهر هو IP منفذ الراوتر RANDD وهو 10.0.2.2، وبذلك يمكننا الدخول عليه عن طريق الـ TELNET والتعرف بواسطته على باقي اجزاء الشبكة، وكالتالي :

2950-24
Research
2960-24TT
InsideSales
2620XM
Marketing
2621XM
Sales
2811
RandD
2950T-24
NewProducts
2960-24TT
OutsideSales

وهكذا يتم التعرف على باقي تفاصيل الشبكة المجهولة بالتتابع وبنفس الكيفية لباقي الاجهزة، وبعد رسمها حسب تصورها تكون النتيجة :

وبما ان الامر SHOW CDP NEIGHBORS DETAIL يستخدم لمعرفة ارقام الـ IP للاجهزة المحيطة بغض النظر اذا ماكان الامر PING ناجحاً ام لا. لذلك يعتبر هذا الامر مفيداً جداً عندما يفشل احد الراوترات في توجيه البيانات المرسلة وذلك بتوضيح اذا ماكان هناك خطأ في اعدادات الـIP لتلك الاجهزة.

اما الامر الآخر والأبسط وهو SHOW CDP NEIGHBORS فيستخدم لغرض عرض معلومات مختصرة عن الاجهزة المرتبطة بشكل مباشر بالجهاز الحالي. محتويات هذه المعلومات تعتمد على نوع الجهاز واصدار نظام التشغيل ولكن اهمها وبشكل عام هي : اسم الجهاز ، نوع منفذ الاتصال لكلا الجهازين ورقمه ، ونوع وفئة الجهاز.

```
HQ>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce    Holdtme    Capability    Platform    Port ID
RandD         Ser 0/0/1         153            R        C2800       Ser 0/2/1
Marketing     Ser 0/0/0         158            R        C2600       Ser 0/0
HQ>
```



ومن الاشياء التي يجب ذكرها وحسب ماتم توضيحه فان تفعيل هذا البروتوكول يعد خطراً على الشبكة، حيث يمكن ألتقاط رسائل الCDP التي يتم تبادلها بشكل افتراضي بين بعض انظمة التشغيل، لذلك اصبح من الضروري معرفة كيفية ايقاف عمل هذا البروتوكول وهو عن طريق الامر:

ROUTER(CONFIG)#NO CDP RUN

هذا الامر يستخدم لايقاف هذه الرسائل بشكل عام ولجميع منافذ الجهاز، اما الامر :

ROUTER(CONFIG-IF)#NO CDP ENABLE

فيستخدم لإيقاف هذه الرسائل بشكل خاص ولمنفذ معين.

هذا اهم مايستحق ذكره في هذا المجال وبشكل مختصر، ولفهم الموضوع بشكل افضل يستحسن التدرب وتجربة هذه الاوامر على شبكة معلومة الاجهزة وطريقة التصميم. بقي اخيرا ان نذكر ان عدد من مصنعي الاجهزة بدأوا بالتحول تدريجيا نحو بروتوكول LLDP (وهو تطوير في عمله لـ CDP) عن طريق الاستغناء عن دعم ارسال المعلومات بواسطته واكتفوا بدعم المعالجة والاستقبال.

مصطلحات في عالم أمن المعلومات

أصبح من الضروري في عالم الشبكات تأمين نقل المعلومات والتأكد من وصولها للهدف والمكان المحدد لها وعدم اطلاع الغير عليها خصوصا المواقع التي فيها تدوال وتحويل الاموال ومواقع التسوق وبعد التطور و التقدم وتطور اساليب المخترقين مثل man in the middle , sniffing حرص مطوري الشبكة العنكبوتية على تحقيق هذا الهدف وحماية هذا البيانات من خلال بعض البروتوكولات والتي سوف تكون حديثنا في هذا المقال مع توضيح بعض المفاهيم والمعاني التي تخص هذه العملية.



Data Integrity

هي صحة البيانات والتأكد من وصولها بدون اخطاء أو نقص في البيانات المنقولة أو عدم وجود أي تلاعب فيها وهي من اهم الاشياء في نظري في أمن المعلومات وهو احد الاساسيات في مثلث الامن والتي تعتمد على تقنيات وبروتوكولات قد نتطرق لها مستقبلا.

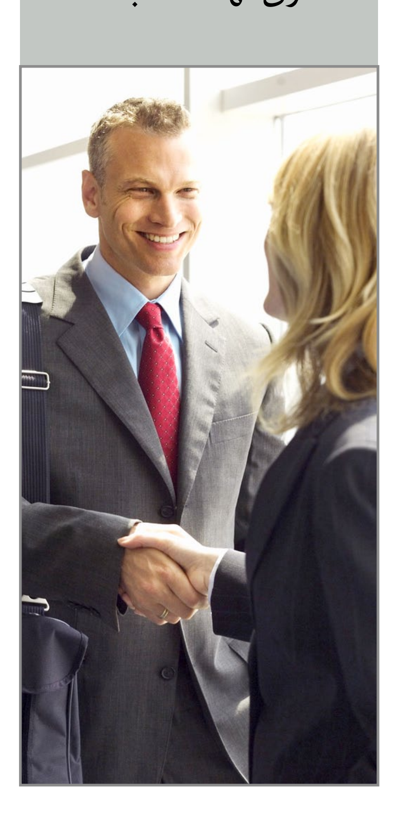
(IPSEC (Internet Protocol Security

أحد المواضيع التي يوجد بها ألتباس كبير هو IPSEC فالكثيرين يظنوا أنه بروتوكول خاص بالسكيورتي لكن الحقيقية هو طريقة تعمل في الطبقة الثالثة Network Layer وهي تقوم بتغلف وتشفير الباكيت وتوثيق البيانات وينقسم الى بروتوكولانAuthentication (Header) AH وهي للتوثيق والتأكد من سلامة الهيدر الخاص بالأيبي والثاني (Encapsulating Security Payload ESP) وهو نفس مهمة الاول لكن خاص بالباكيت نفسها .

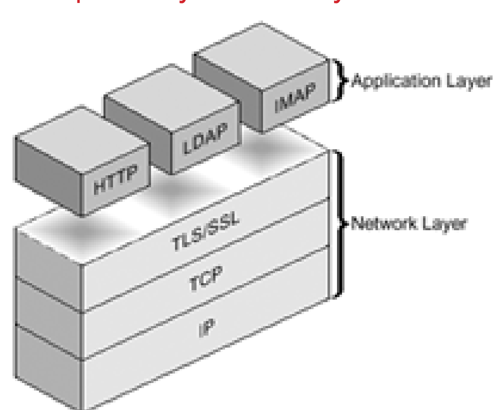


SNIFFING

المعروف بمحلل البكيت أومحلل الشبكة وهو برنامج أو قطعة من جهاز الكمبيوتر تقوم باعتراض البـاكـيـت او البيانات خلال مرورها خلال الاسلاك أو الشبكة اللاسلكية ومن امثلة البرامج المستخدمة البرنامج المشهور wire shark و Ettercap .



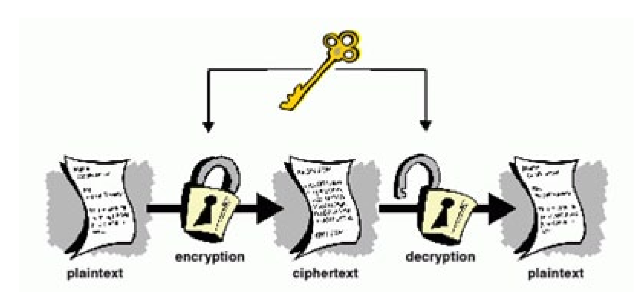
Transport Layer Security (TLS)



طبقة امن النقل وهو بروتوكول يضمن خصوصية التنقل بين الطبقات والمستخدم على شبكة الانترنت ويضمن عدم وجود طرف ثالث يحاول التصنت والتجسس وتستخدم عددا من البروتوكولات لتاسيس اتصال آمن منها HTTP, IMAP, POP3, و SMTP.

Symmetric-key algorithms

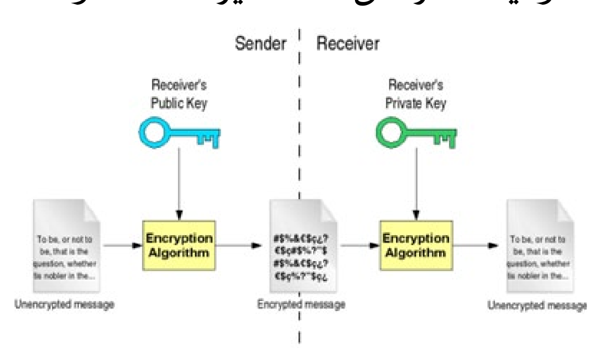
خورزمية المفتاح المتماثل سمية بهذا الاسم لتطابق مفاتيح التشفير وفك التشفير عن المرسل والمستقبل وهي تمثل كلمة سر مشتركة بين الطرفين.



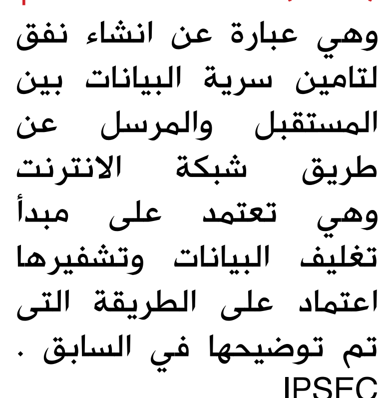
Asymmetric key algorithms

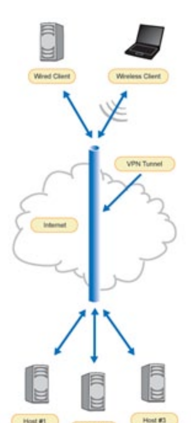
خوارزمية الغير متماثلة وفيها تختلف مفاتيح التشفير عن مفاتيح فك التشفير بين المرسل والمستقبل وتنقسم الى قسمين من المفايتح Private key وهو المفتاح الذي لايعرفه إلا الجهاز المرسل أو المستقبل والذي يستخدم لفك التشفير.

Public keyوهو المفتاح الذي يرسل للطرف الآخر والذي يعتمد عليه في عملية التشفير بحيث يكون مفتاح الـ Private هو المفتاح الوحيد القادر على فك تشفير هذه المعلومات.



A virtual private network (VPN)





وهي عبارة عن انشاء نفق لتامين سرية البيانات بين المستقبل والمرسل عن طريق شبكة الانترنت وهي تعتمد على مبدأ تغليف البيانات وتشفيرها اعتماد على الطريقة التى تم توضيحها في السابق . IPSEC

Plain text

هو النص الواضح الغير مشفر وهو لا يحتاج لمعاجة أوتحويل وقابل للقراءة

cyphertext او Cipher text

هو نتيجة التشفير التي أجريت على النص الواضح باستخدام خوارزمية ما، والشفرات و النص المشفر هو المعروف أيضا باسم معلومات مشفرة أو مرمزة لأنه يحتوي على شكل مشفر من الأصل الغير قابل للقراءة من قبل فك التشفير، و معكوس التشفير هو عملية تحويل النص المشفر إلى نص غير مشفر قابل للقراءة . ويحتاج لبرنامج الشفرات المناسبة لفك تشفيرها .

هذا واللّه أعلم وان شاء اللّه نتابع في الاعداد القادمة بشرح اكثر عن هذا العلم الرائع .

Magazine NetworkSet

First Arabic Magazine for Networks

معنى جديد لعالم الشبكات في سماء اللغة العربية

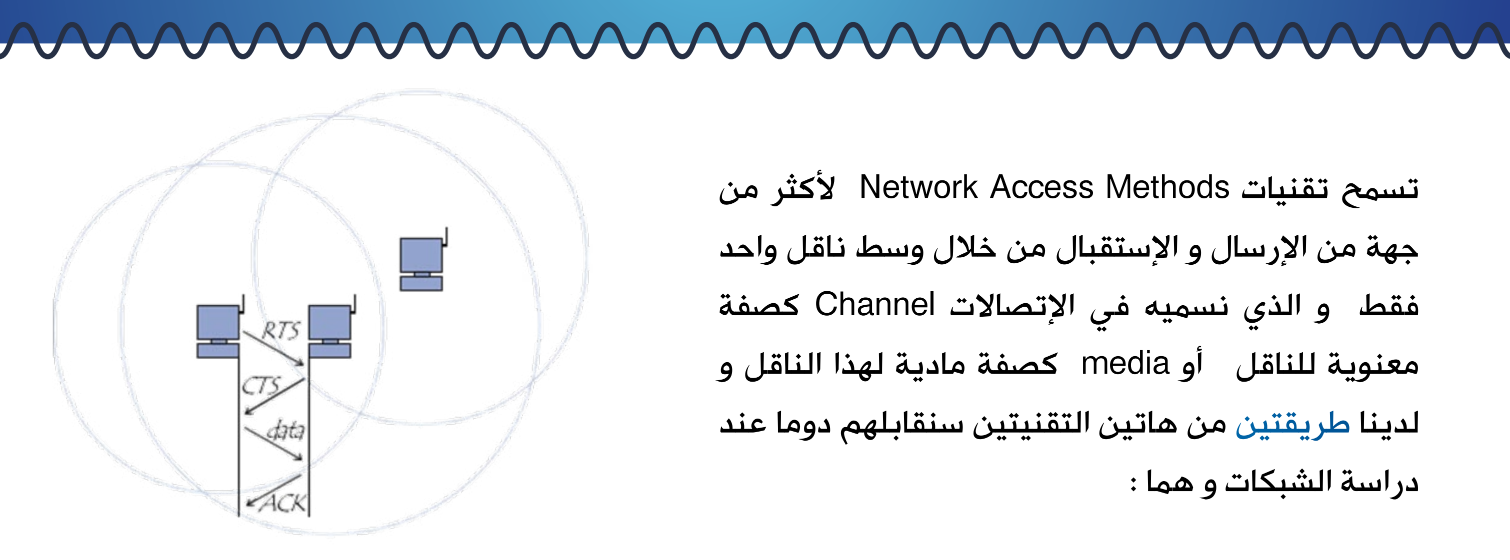








CSMA/CA vs CSMA/CD

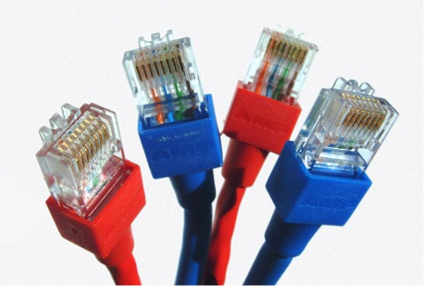


تسمح تقنيات Network Access Methods لأكثر من جهة من الإرسال و الإستقبال من خلال وسط ناقل واحد فقط و الذي نسميه في الإتصالات Channel كصفة معنوية للناقل أو media كصفة مادية لهذا الناقل و لدينا طريقتين من هاتين التقنيتين سنقابلهم دوما عند دراسة الشبكات و هما :

arrier sense multiple access with collision avoidance أو CSMA/CA أو تحسس القناة مع تفادي التصادم و هي تختص بالشبكات اللاسلكية مثل شبكات الواي فاي و بعض تقنيات الشبكات اللاسلكية الأخري مثل WirelessHARTPAN وZigbe و الذين ينتمون الي شبكات IEEE 802.15.4 PAN	كذلك يتم استخدامها في لشبكات السلكية خارج نطاق الإيثرنت مثل Apple's LocalTalk وBus networks كذلك تستخدمها بعض أشكال الشبكات التي تعتمد علي البنية الشبكية للمنازل و التي لا تتطلب وجود QOS مثل power lines - phone lines – coaxial cables	و الثانية هي CSMA/CD Carrier sense multiple access with collision detectionأو تحسس القناة مع اكتشاف التصادم و و تستخدم في الشبكات السلكية

و كلاهما CSMA/CD – CSMA/CA ينتميان الي طرق الوصول المعتمدة علي الباكات Packet based أو Network Access Methods علي عكس FDMA و CDMA و غيرهم حيث ينتمون الي Channel based

و لقد أعطي صاحب كتاب CWTS "أخصائي مبيعات الشبكات اللاسلكية" مثال رائع عنهما فيقول عن CSMA/CD

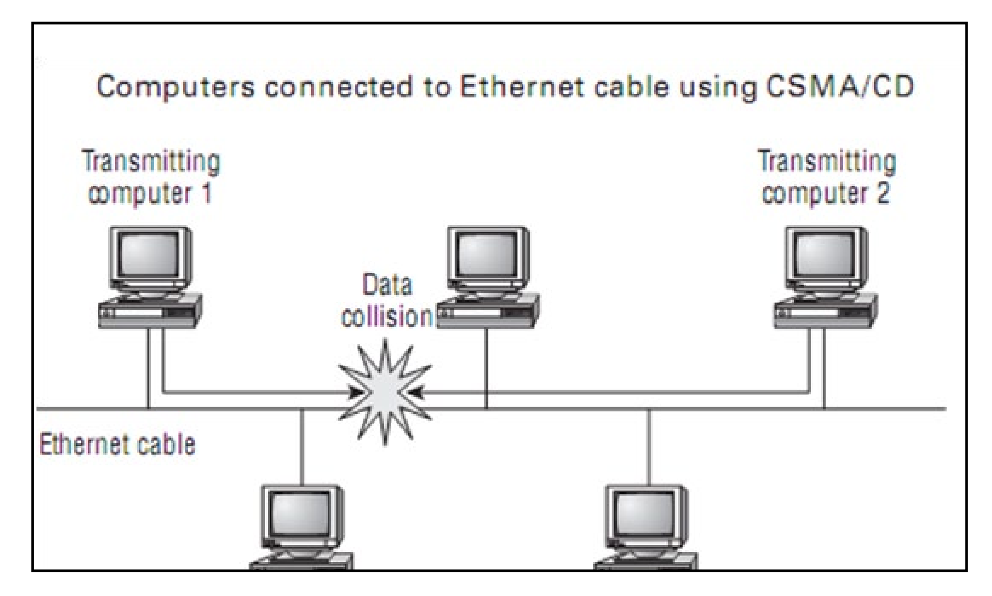


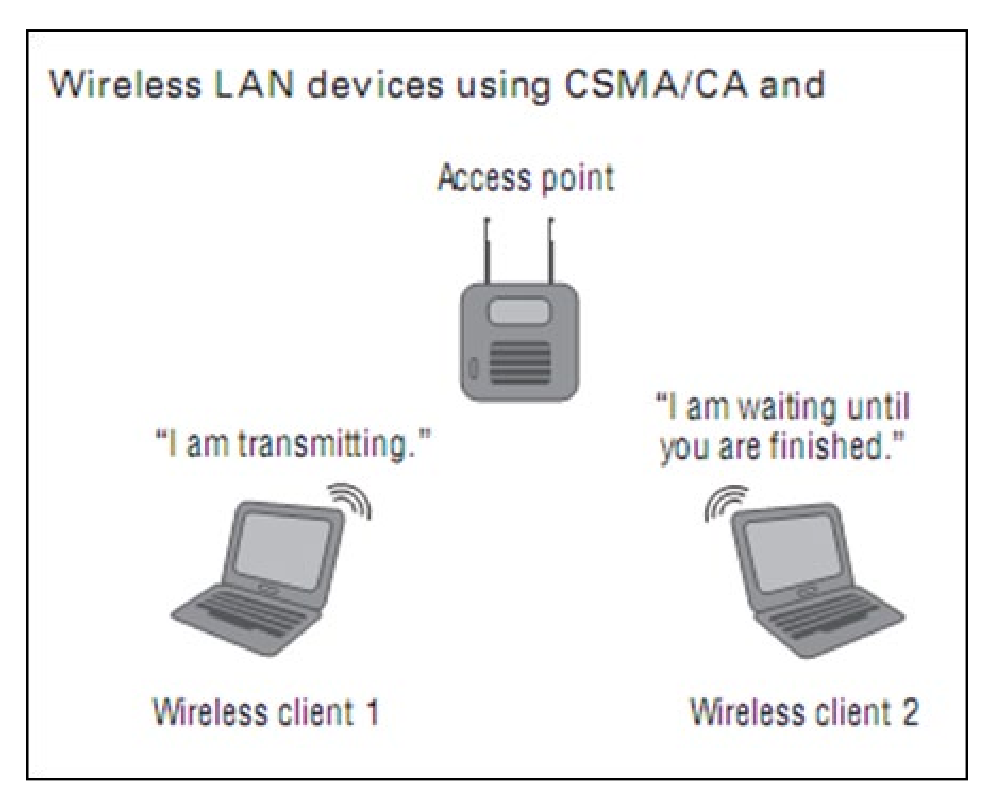
افترض ان عدة أشخاص في اجتماع و تدور بينهم محادثة و كل منهم لدية فرصة للحديث و الكل يستمع الي الشخص الذي يتكلم حاليا و الكل يتحين فرصة الكلام بعده و هذا يوزاي Carrier Sense اي تحسس الوسط و الإستماع اليه و لكي يستطيع الجميع فهم الحديث فلا يسمح سوي لشخص واحد فقط بالتحدث في نفس الوقت و هذا يسمي Multiple Access MA

عندما ينتهي المتحدث تحدث برهة صمت ثم يحاول آخر أو آخرون أن يتحدثوا و في حالة قام أكثر من شخص

بالتحدث يحدث تصادم فيصمتوا ليسمح لواحد فقط و هذا هو Collision Detection CD

أما في حالة CSMA/ CA فإنه قد افترض أن الأمر و كأنك في محاضرة و بعد انتهاء المحاضر يطلب منهم الإستفسار عن أي شيء في المحاضرة و الكل يتهيأ للإستفسار عن بعض ما ورد فيها و هذا هو MA Multiple Access يقوم أحد الأشخاص بالتلفت يمينا و يسارا ليري هل من أحد قام ليلقي السؤال و هذا هو Carrier Sense وعندما لا يجد أحد يقوم بإلقاء السؤال و لكن الباقون بإنتظاره حتي ينتهي ليلقي أحدهم السؤال و هذا Collision Avoidance

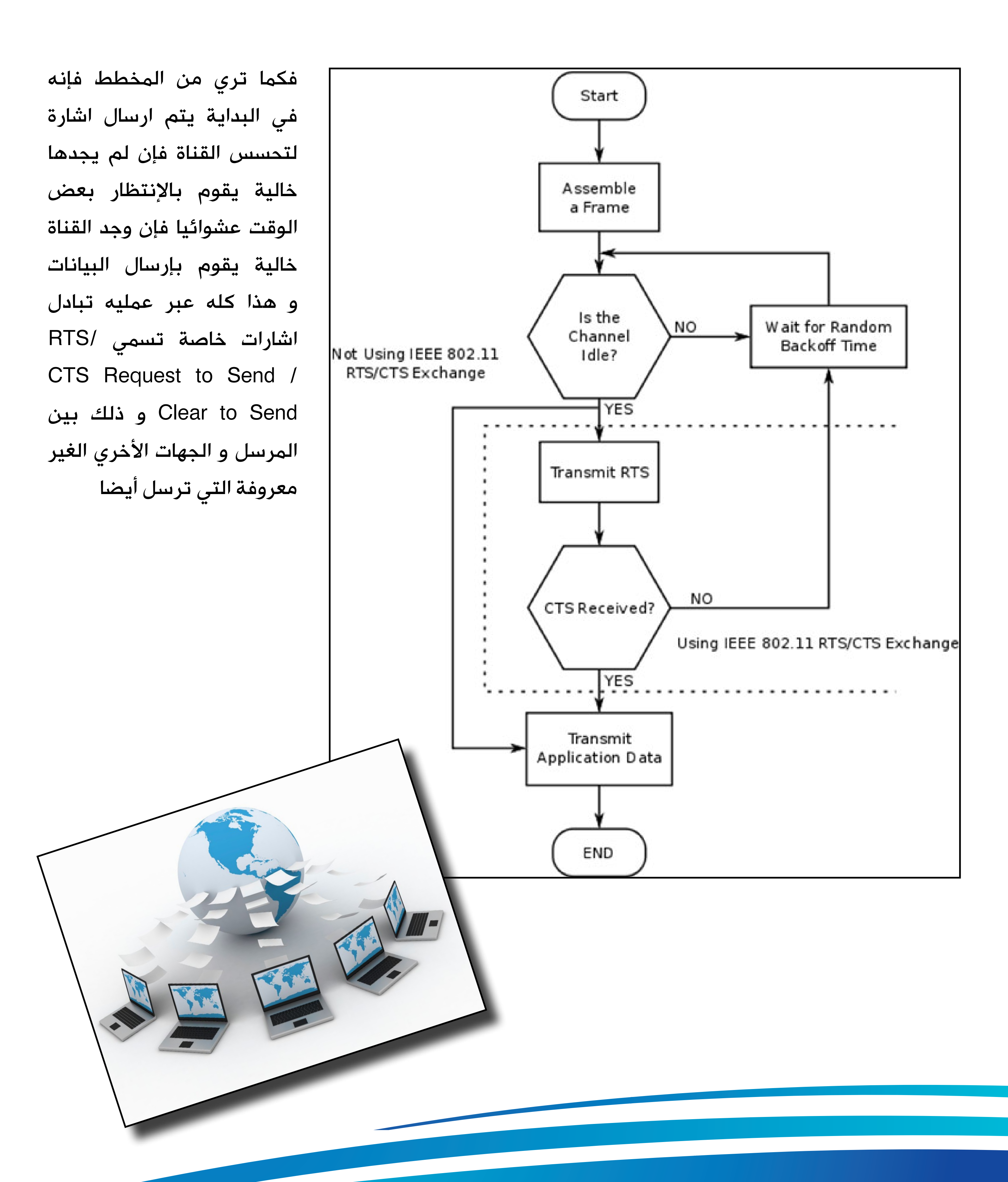


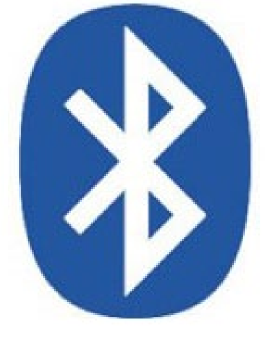


طريقة العمل

تعتمد شبكات الإيثرنت علي امكانية اكتشاف التصادمات أثناء التراسل علي الوسط الناقل media و ذلك اعتمادا علي CSMA/CD و لكن في الشبكات اللاسلكية لا تستطيع الأجهزة التصنت علي القناة في نفس وقت الإرسال و حيث أنه من الطبيعي أن يقوم أكثر من جهاز في نفس الوقت بالتراسل عبر الأكسس بوينت في الشبكات اللاسلكية فإن حدوث تصادم لا يخدم البيانات و يجعلها عرضة للضياع علي عكش الشبكات السلكية الذي يكتشف التصادم فيقوم بإعادة ارسال البيانات و يرسل اشارة Jam يخبر فيها الأطراف الأخري بعدم التعامل مع البيانات التي تصادمت لكونها غير صالحة اذن فالحل هو عدم التصادم .

فكما تري من المخطط فإنه في البداية يتم ارسال اشارة لتحسس القناة فإن لم يجدها خالية يقوم بالإنتظار بعض الوقت عشوائيا فإن وجد القناة خالية يقوم بإرسال البيانات و هذا كله عبر عمليه تبادل اشارات خاصة تسمي /RTS CTS Request to Send / Clear to Send و ذلك بين المرسل و الجهات الأخري الغير معروفة التي ترسل أيضا





Bluetooth

بما ان كلمة بلوتوث اصبحت منتشرة بشكل واسع واصبح هذا المصطلح في كل مجال ، بل لايكاد يخلو مكان من جهاز يعمل بهذه التقنيةفنراها في الهواتف المتنقلة وفي الكمبيوترات وفي البيوت والمستشفيات والسيارات وغيرها ، لذلك اصبح من الضروري لجميع المهتمين بمجال الشبكات ان يدركوا الية وطريقة عمل وخصائص وتركيب هذه الشبكةوليس مجرد استعمالها كحال المستخدمين العاديين لهذه التقنية. هذا مانحن بصدد معرفته في مقالنا هذا وساحاول بقدر الامكان التركيز على المعلومات التي تخص مجال الشبكات. لذلك دعونا نبدا اولا بالتعرف على معلومات اساسية عنها.

فالبلوتوث هو احد تقنيات الشبكات اللاسلكية يستخدم في تبادل البيانات بين الاجهزة (gadgets) ضمن مدى قصير نسبيا حيث ان هذه التقنية جاءت لتحل محل تقنية الاشعة تحت الحمراء IrDA فهي لاتتطلب ان تكون الاجهزة المقترنة باتجاهين متقابلين بالاضافة الى امكانية الاتصال بين جهاز وعدة اجهزة اخرى في نفس الوقت.تـُعرف تقنية البلوتوث بالمعيار IEEE 802.15 وتصنف من ضمن الشبكات الشخصية PAN.

بدأ العمل في هذا المشروع من قبل شركة اريكسون السويدية عام 1994 واشتق مصطلح البلوتوث من اسم الملك الدنماركي Harald Blaatand والذي قام بتوحيد الدنمارك والنرويج حيث ان كلمة Blaatand تعني بالانكليزية Bluetooth ، لهذا تم اطلاق هذه التسمية على البلوتوث كونه وحد بروتوكولات الاتصالات تحت معيار عالمي واحد. كذلك شعار البلوتوث اشتق من الاحرف الاولى من اسم الملك، فحسب الاحرف الرونية القديمة فحرف H يمثل بالرمز وحرف B يمثل بالرمز وعند دمجهما يتكون شعار البلوتوث.

معلومات تقنية عن البلوتوث

يعمل البلوتوث ضمن حزمة ISM بتردد 2.4كيكاهيرتز حيث تكون الحزمة مقسمة الى 79 قناة وبعرض حزمة 1 ميكاهيرتز لكل منها.

ونظرا لاستعمال البلوتوث غالبا في الاجهزة المتنقلة لذلك يجب ان يكون استهلاك هذه الاجهزة للطاقة عند استعمال هذه التقنية قليلوهذا الذي جعل مدى الارسال بين اجهزة البلوتوث قصير نسبيا فهو لايتعدى 10 امتار عندما تكون قدرة الارسال 0db او 1 ملي واط ، ويمكن زيادة هذه المسافة الى 100 متر بزيادة قدرة الارسال الى 20db في الاماكن المفتوحة ويتغير هذا المدى حسب ظروف الارسال ووجود الحواجز. وحسب الجدول التالي :

الفئة	اعلى قدرة للارسال dBm	اعلى قدرة للارسال mW	المدى (بشكل تقريبي)
فئة 1 (class 1)	20	100	100 متر
فئة 2 (class 2)	4	2.5	10 متر
فئة 3 (class 3)	0	1	5 متر

ومن الجدير بالذكر ان الجهاز من فئة 2 يمكن ان يرفع مدى ارساله عندما يتصل مع جهاز من فئة 1، هذا التغير يحدثعن طريق جهاز فئة 1 بزيادة امكانية التحسس للاشارة الضعيفة المرسلة من جهاز فئة 2 عند الاستقبال وكذلك بزيادة القدرة عند الارسال.



البلوتوث مقابل التقنيات الأخرى

Category	Home-RF (1.09)	802.11	Bluetooth	IrDA (AIR)
Market	Home WLAN	WLAN	Cable	Cable
Technology	RF: 2.4 GHz FHSS	RF: 2.4 GHz FHSS/DSSS	RF: 2.4 GHz FHSS	Optical 850 nm
Power	20dBm	20dBm	0/20dBm	?
Symbol Rate	0.8/1.6 M	11M	1M	4M/115K
Distance	50m	30-100 m	0-10m/100 m	0-3m/5m
Topology	128 devices CSMA	128 devices CSMA	8 devices Pt to MP	10 devices Pt to MP
Security	Optional	Optional WEP	Authentication, Key, mgmt, Encryption	Application Layer
Cost	Low	High	Low	Low

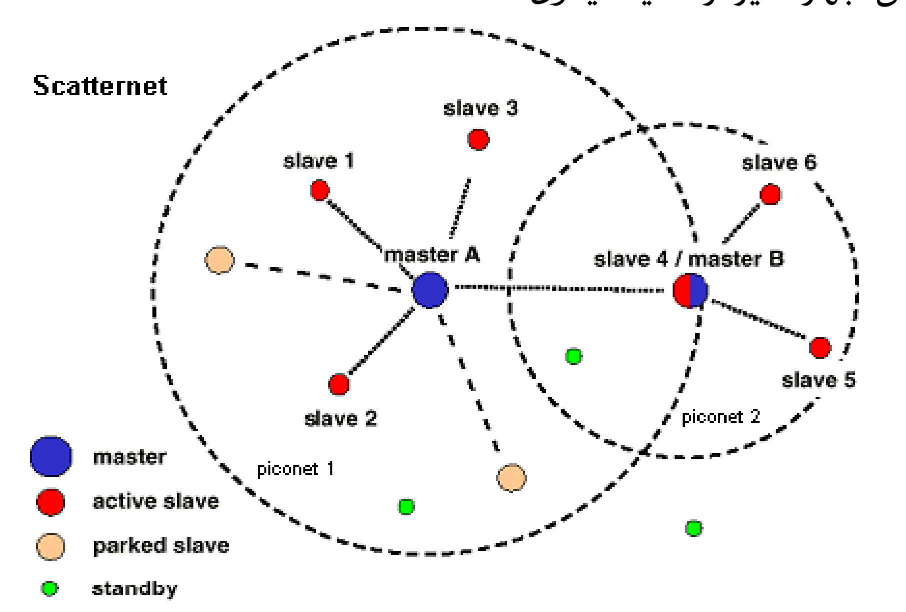
معمارية البلوتوث

تكون عملية الاتصال في شبكات البلوتوث بين الاجهزة بطريقة السيرفر والكلاينت حيث ان الجهاز الواحد ممكن ان ياخذ احد الوضعين. وعند ربط مجموعة من هذه الاجهزة تتكون شبكة من نوع Adhoc تسمى البيكونت Piconet.

شبكة البيكونت تحتوي على 8 اجهزة كحد اقصى وهذا يعني وجود جهاز واحد يعمل كسيرفر وباقي الاجهزة الاخرى تعمل ككلاينت (بعض المصادر تسميها master و slave او رئيسي وثانوي). وتقوم هذه الكلاينت بمزامنة توقيتها الداخلي وتسلسل القفز بين الترددات (hopping sequence) مع السيرفر. حيث يمكن ان تحتوي الشبكة على اكثر من 7 اجهزة كلاينت ولكن فقط 7 منها تكون فعالة في الوقت الواحد والاخرى تكون في حالة وقوف مؤقت parked state. والتي يقتصر نشاطها على عملية التزامن ولايمكنها المشاركة فعليا في عملية الاتصال مالم تنتقل الى الحالة النشطة وتحول احد الاجهزة النشطة الى حالة التوقف المؤقت.

عملية انشاء الاتصال تتم بواسطة الجهاز السيرفر - يمكن للجهاز الكلاينت ان يعمل طلب للتحول الى جهاز سيرفر- حيث يكون هذا السيرفر هو بمثابة البوابة لجميع الكلاينت فلا يمكن الاتصال بين كلاينت واخر الا عن طريقه.

عند تجمع عدد من البيكونت متداخلة في تغطيتها مع بعضها تتكون شبكة تسمى بالـ Scatternet. في هذه الشبكة يمكن للجهاز الواحد ان يكون سيرفر في شبكة بيكونت ما وكلاينت في شبكة اخرى او كلاينت في اكثر من شبكة بيكونت.



عملية اعداد الاتصال في البلوتوث :

أي جهاز بلوتوث اثناء عملية الاستكشاف للاجهزة الموجودة في المحيط يقوم بارسال هذه المعلومات :

- اسم الجهاز.
- فئة الجهاز.
- الخدمات التي يدعمها.
- معلومات تقنية (مميزات الجهاز، المصنع، ومعلومات اخرى).

كل جهاز يستعمل تقنية البلوتوث لديه عنوان ثابت وخاص بذلك الجهاز كعنوان MAC في اجهزة الكمبيوتر يسمى (BD_ADDR)ويتكون من 48 بت ويحدده جمعية مهندسي الكهرباء والألكترونيات (IEEE). غير ان هذه الارقام لاتظهر في عملية البحث فبدلا من ذلك يتم اظهار اسماء اما محددة من قبل الشركة المصنعة للجهاز او محددة مسبقا من قبل المستخدم.

فعندما يتقارب جهازا بلوتوث من بعضهما البعض،فإن حديث إلكتروني يجري لمعرفة إن كانت هناك بيانات للمشاركة او اذا على الجهاز الأول التحكم في الجهاز الثاني وهذا الامر كله يجري بدون الحاجة إلىضغط اي زر او إصدار اي امر.

فهذا الحديث الإلكتروني سيأخذ مجراه بشكل تلقائي وعندما يتم الاتصال مابين الجهازين فإنه يتم تكوين شبكة معينة مابين الجهازين،وتقوم أنظمة بلوتوث بعدئذ بإنشاء شبكة شخصية قدتمتد لغرفة كاملة او تمتد لمتراو اقل. وعندما يتم تكوين الشبكة الشخصية فإن الجهازين يقومان بتغيير التردد بطريقة واحدة وفي وقت واحد حتى لايتم التداخل مع شبكات شخصية أخرىالتي قد تكون موجودة في نفس المكان.

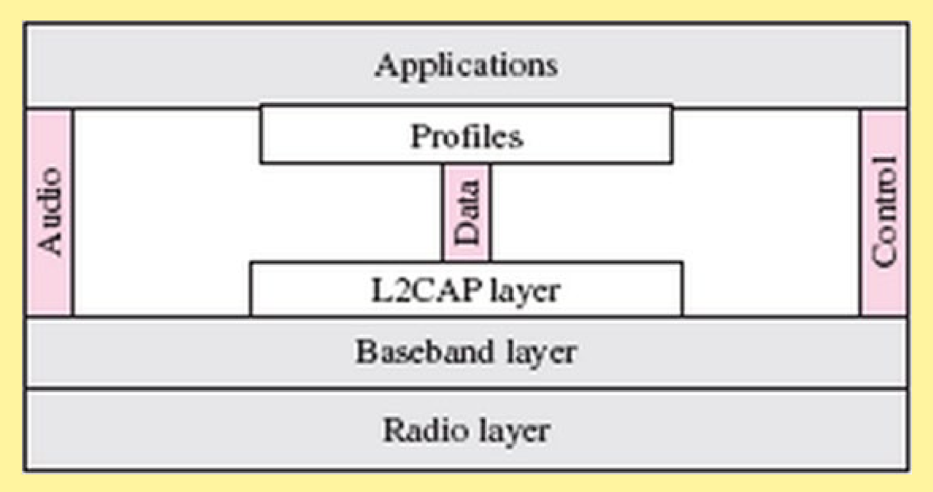
آلية الاقتران بين اجهزة البلوتوث :

هناك نوعين من الاقتران بين هذه الاجهزة ففي الاجهزة التي تعمل باصدار 2.0 وماقبلها يتطلب ان يدخل كلا الجهازين رمز PIN، ولكي ينجح الاتصال فيجب ان يكون كلا الرقمين المدخلين متطابقين والا فالاتصال يلغى. وبما انه ليست جميع الاجهزة تستطيع ادخال جميع رموز PIN مثل سماعات الراس التي تعمل بهذه التقنية لذلكفإن مثل هذه الاجهزة تحتوي على رقم مبرمج على الجهاز مسبقا وغالبا مايكون اما «0000» او «1234» . وبعضها تستطيع ادخال فقط ارقام مثل الهواتف النقالة وبعضها تستطيع ادخال جميع الرموز من نوع UTF-8كما في الاجهزة الذكية والكمبيوترات. اما الاجهزة التي تعمل باصدار بلوتوث 2.1 ومابعدها فالجهاز قد لايحتاج الى تدخل المستخدم او قد يحتاج فقط لتاكيد الاتصال او الغائه كما يحدث في بعض الاجهزة التي تحتوي على ازرار قليلة مثل سماعات الرأس. وبعض الاجهزة تقوم بعرض رقم من 6 خانات في كلا الجهازين المقترنين لكي يقوم المستخدم بمقارنة الرقمين ثم يقرر بقبول الاتصال او رفضه.



طبقات البلوتوث

يتكون البلوتوث من عدة طبقات تختلف نوعا ما عن تلك الطبقات الخاصة بـOSI Model . حيث انها تبدا بالطبقة الراديوية وتنتهي بالتطبيقات والتي تشترك بها مع ModelOSI.



الطبقة الراديوية

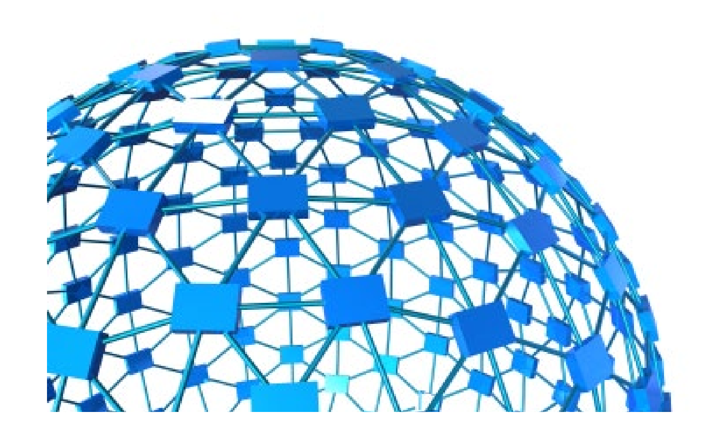
Radio Layer

هذه الطبقة تكافئ الطبقة الاولىPhysical Layer في طبقات OSI Model، فكما ان الطبقة الفيزيائية هي المسؤولة عن ارسال البيانات عبر الوسط الناقل في طبقات OSI Modelفكذلك هي الطبقة الراديوية مسؤولة عن عملية الارسال في البلوتوث، وكما ذكرت فإن عملية الارسال تكون لاسلكيا وعبر موجات الراديو لكن بطاقة ارسال قليلة حيث يستخدم حزمة الارسال 2.4 كيكاهيرتز وتكون الحزمة مقسمة الى 79 قناة وبعرض حزمة 1 ميكاهيرتز لكل منها و لمعرفة ترددات كل قناة (بالميكاهيرتز) يمكن استخدام الصيغة الرياضية الآتية :

ترددالموجةالحاملة)) fc= 2402 + n حيثان : n = 0،1، 2 ، 3 ،...................78

فعلىسبيل المثال تردد الاشارة الحاملة للقناة الاولى =2402 ميكاهيرتز و القناة الثانية = 2403 ميكاهيرتز و هكذا.

في عملية تحويل الارقام الى اشارات ،يستخدم البلوتوث في عملية التضمين نسخة معقدة و متطورة من FSK تدعى GFSK (وهو عبارة عن FSK مع Gaussian bandwidth filtering). ايضا بما ان البلوتوث يحتاج الى مستوى عالي من الامن وكذلك فإن العديد من التقنيات تستخدم حزمة الارسال ISM لذلك اصبح من الضروري ايجاد طريقة ارسال للبلوتوث تمنع التداخل بين ترددات



هذه الاجهزة وتتمتع بدرجة عالية من الامن لذلك يستخدم البلوتوث طريقة الارسال المعروفة بـ FHSS (frequency-hopping spread spectrum)وهي تعني ان البلوتوث يقفز في تردداته 1600 مرة في الثانية الواحدة او بمعنى اخ رفان كل جهاز بلوتوث يغير تردد التضمين الخاص به 1600 مرة في الثانية الواحدة وكما نعرف ان التردد هو مقلوب الزمن لهذا فان زمن استخدام الجهاز لكل تردد لا يتعدى 625 مايكروثانية او (1\1600) ثانية قبل ان يغير تردده الى تردد اخر. ويسمى هذا الزمن بزمن الاقامة او dwell time.

طبقة الحزمة الاساسية

هذه الطبقة تكافئ تقريبا طبقة MAC الثانوية في طبقات OSI. تستخدم طريقة الوصول للقناة المعروفة بـ TDMA، وتعني ان الجهاز السيرفر والكلاينت يتصلان مع بعضهما باستعمال طريقة تقسيم الزمن، حيث ان جزء الزمن slot المخصصtime لكل جهاز هو نفسه زمن الاقامة dwell time الذي ذكرته سابقا ويساوي 625 مايكروثانية. هذا يعني ان خلال هذا الزمن تردد واحد يمكن استخدامه بحيث يمكن للمرسل ان يرسل فريم الى الكلاينت او الكلاينت يرسل فريم الى السيرفر ولايوجد هناك ارسال من كلاينت الى كلاينت اخر.

في الحقيقة تقنية البلوتوث تستخدم صيغة معينة من TDMA تسمى -TDD TDMA

((Time DivisionDuplex TDMA

وهومن نوع الاتصال المزدوجHalf Duplexويعني ان المرسل والمستقبل كلاهما يقومان بالارسال والاستقبال ولكن ليس في نفس الوقت.

عملية الارسال في شبكة البيكونت التي تحتوي على كلاينت واحدتكون بسيطة للغاية. حيث يتم تقسيم الزمن الى اجزاء من 625 مايكروثانية لكل منها،يستخدم السيرفرالاجزاء ذات الارقام الزوجية ويستخدم الكلاينت الاجزاء ذات الارقام الفردية، وهذا يعني ان السيرفر يرسل والكلاينت يستقبل في الجزء رقم 0 والسيرفر يستقبل والكلاينت يرسل في الجزء رقم 1 وهكذا تعاد العملية.

اما اذا كانت شبكة البيكونت تحتوي على اكثر من كلاينت فالعملية اكثر تعقيدا فالسيرفر كذلك يرسل في الاجزاء الزوجية وجميع الكلاينت تستمع للسيرفر عند ارساله ولكن واحد منهم فقط يرسل في الجزء الفردي وحسب العنوان المرسل من قبل السيرفر في الجزء الزوجي السابق.

يدعم البلوتوث نوعين من الربط عند الاتصال بين السيرفر والكلاينت هما SCO وACL.

يُستخدم SCOوا Synchronous Connection-Orientedlink في نقل الصوت بين الاجهزة حيث تكون السرعة في نقل البيانات (latency) اكثر اهمية من دقة البيانات المستلمة(integrity) لذلك فعندما تصل البيانات غير صحيحة او تالفة فلن يتم اعادة الارسال لذلك الفريم. في هذا الربط الكلاينت يمكن ان ينشأ 3 قنوات اتصال SCO كحد اقصى مع السيرفر لنقل الصوت بشكل رقمي PCM وبسرعة 64 kbps عبر كل قناة.

اماACL او Asynchronous ConnectionLess link فيُستخدم في نقل البيانات بين الاجهزة عندما تكون دقة البيانات المستلمة وخلوها من الاخطاء اكثر اهمية من سرعة النقل. سرعة النقل في هذا النوع من الربط تصل الى 721 kbps كحد اقصى.

صيغة الفريم في طبقة baseband تكون على 3 انواع -one-slot ، three slot او five-slot. سوف لن اتطرق الى تفاصيل هذه الانواع ولكن يكفي ان نعرف صيغة الفريم بصورة عامة وهي على النحو الاتي :

Access code (72 bits)	Packet header (54 bits)	Payload (0-2754 bits)

Access code : هذا الحقل خاص يحتوي على المعلومات الخاصة بعملية المزامنة وكذلك المعلومات التي يستطيعها السيرفر تمييز الفريم من أي شبكة بيكونت قادم.

- Packet header : هذا الحقل يعاد ارساله 3 مرات بشكل متكرر ويتكون من 18 bits في كل عملية ارسال. هذه الطريقة تستخدم في تصحيح الخطأ في الفريم كون الارسال يكون لاسلكيا فعند استقبال الثلاث رسائل يتم مقارنة هذه الرسائل مع بعضها فاذا لم يكن هناك اختلاف بين هذه الرسائل يتم قبول الفريم. اما اذا كان هناك اختلاف فيتم اعتبار الرسالتين المتطابقتين هي الصحيحة. كل رسالة او قسم من هذا الحقل يتكون من :

- Address : يتكون هذا الحقل من 3bits حيث ان هناك 7 اجهزة كلاينت فعندما يكون هذا الرقم 0 هذا يعني ان الارسال هو Broadcast أي من السيرفر الى جميع الكلاينت.
- Type : يتكون هذا الحقل من 4 bits ويُعرف نوع البيانات القادمة من الطبقات العليا.
- F : هذا الحقل هو 1 bit خاص بعملية flow control. عندما يكون 1 فهذا يعني ان الجهاز غير قادر على استقبال بيانات اكثر.
- A : هذا الحقل هو ايضا 1bitخاص بعملية الابلاغ بالاستلام acknowledgment.
- S : يتكون من 1 bit وهو يحمل تسلسل الفريم sequence number.
- HEC : يتكون من 8 bit وهو المسؤول عن عملية تصحيح الاخطاء في الرسائل الثلاث بشكل خاص وليس في كامل الفريم كما ذكرت سابقا.

- Payload : ويحمل هذا الحقل البيانات المراد ارسالها او معلومات السيطرة القادمة من الطبقات العليا.

طبقة L2CAP او Logical Link Control and Adaptation Protocol :

هذه الطبقة تكافئ تقريبا طبقة LLC الثانوية في طبقات OSI. وهي مسؤولة عن عملية الـ multiplexing وبمعنى اخر فهي تقوم باستقبال البيانات من الطبقات العليا وتحولها الى فريم ومن ثم تسلمها الى طبقة baseband هذا عند المرسل اما عند المستقبل فالعملية بالعكس. ايضامن مهامها هو عملية تجزئة الباكيت واعادة تجميعها Segmentation and Reassembly وكذلك من مهامها هو (QoS(Quality of Service.

اضافة الى ذلك فهي تقوم بعملية ادارة المجموعاتوتعني ان عدد من الكلاينت تستطيع ان تعمل مجموعة Multicast لاستلام رسائل خاصة بها من السيرفر.

الطبقات الاخرى المتبقية تكون مسؤولة عن اعدادات الاتصال وعملية انشاء الاتصال وتطبيق خطوات الامن والتوثيق في الاقتران وانهاء الاتصال، كذلك تحتوي على البرامج والتطبيقات التي تسيطر على عملية تبادل البيانات وترجمتها واظهارها.

والان بعد ان اخذنا لمحة سريعة عن هذه التقنية وعرفنا مميزاتها نستطيع ان نقول ان هذه التقنية ليست خالية من المساوئ مثلها مثل كل التقنيات فلكل تقنية مساوئها ومميزاتها ولكن كون هذه التقنية من ابسط وافضل التقنيات في خدماتها وتكلفتها الواطئة جعلها الاكثر انتشارا.



خالد عوض

الـشـبـكـات فـي عـالـم آبــل

كثيرا من يذكر سيسكو ومنتجاتها عندما يكون الحديث عن شبكات الحاسب الآلي. وتارةً ما نتطرق لمنتجات جونيير وتقنياتها ، ونذكر ميكروسفت عندما نتكلم عن الأنظمة المتعلقة بالشبكة. ولكن في هذا المقال سنتتطرق لشي جديد للأغلبية في مجال الشبكات. آلا وهو (الشبكات في عالم آبل).

إن الكثير منا يظن أن ما يتعلق بالشبكات في بيئة الويندوز يكون نفسه الموجود في منتجات آبل. ولكن في الواقع العملي الأمور تختلف عما تتصور ، فكما نلاحظ أن شركة آبل دائماً ما تستقيل بأنظمتها وتقنياتها فدعونا نتعرف على عالمها.

في منتصف الثمانيات قدمت Apple معمارية خاصة بها لربط مجموعة من المستخدمين لتكوين شبكة. حيث تضمنت تلك المعمارية عائلة من التقنيات التالية:

- AppleTalk
- LocalTalk
- AppleShare
- EtherTalk
- TokenTalk

حيث أن بروتوكول AppleTalk هي النسخة الخاصة بأجهزة Apple MAC التي أطلقت عام 1985 م . و صدرت بأسم AppleTalk Phase 1 وبعد مرور فترة من الزمن طورت آبل هذه النسخة وأطلقتها بأسم AppleTalk Phase 2 . في بداية الأمر كان هذا البروتوكول مقتصر إستخدامة على أجهزة Apple Mac وبعدها توسع وتطور ليدعم منتجات أخرى حتى أشتهر وأطلق عليه LocalTalk ليشمل هذا الأسم عملية التشبيك المستخدمة لهذا البروتوكل ككل.

أما عن المنتج الاخر وهو AppleShare الذي أطلقته



آبل ليكون الغرض الأساسي منه العمل كـ File Serverمن خلال بروتوكول يعرف بـ Apple Filing Protocol (AFP) . ولكن مع مرور الزمن قررت آبل أن تطور هذا المنتج ليدعم تقنيات أخرى فقاموا بأضافة خاصية الوصول للطابعات عبر الـ Print Server وذلك بواسطة بروتوكول PAP . وأضافوا مميزات أخرى ومنها Web Server و Mail Server . وبعدها أدركت آبل أنها بحاجة لوضع ميزة تمكن أجهزتها من الوصل لمصادر أجهزة أخرى تعمل تحت بيئة الويندوز ، فقاموا بأبتكار تقنية SMB CIFS .

أما EtherTalk)) فهو أحد معايير IEEE 802.3 . وهو أحد البروتوكولات التى قامت شركة آبل بتطويره لصالح كروت الشبكة بحيث تتوافق مع أنواع مختلفة من الكابلات ومنها Coaxial و Twisted Pair و Fiber-Optic . وكما أن هذه الكروت يطلق عليها Ethernet NB او Ethernet LC . ويتوفر نوعاً خارجياً من هذه الكروت يوصل بمنفذ SCSI . وهذه البطاقات التي تعمل تحت هذا المعيار تسمح لأجهزة Apple Mac بالإنضمام لشبكة Ethernet وكما أنها متوافقة أيضاً مع AppleTalk Phase 2 الذي ذكرناه سابقاً وذلك بواسطة البرنامج المدمج في هذه البطاقات.

وبعد أن تعرفنا على بعض المعلومات عن الشبكات في عالم آبل . لاشك أن من الضروري أن نذكر البروتوكولات المهمة التي تعمل في هذه الشبكات كونها عصب التواصل عبر الأجهزة . فلنترك لكم الجدول التالي يوضح لكم بعض البروتوكولات المهمة في عالم شبكات آبل والغرض منها :

البروتوكول	الإسم الكامل	وظيفته
UDP	**Datagram Delivery Protocol**	البروتوكول المسؤول عن توصيل **Datagram** بين أجهزة الشبكة .
NBP	**Name Binding Protocol**	بروتوكول يمنح أي خدمة على الشبكة بتسجيل إسماً لها عند بداية عملها حتى تستطيع الأجهزة الأخرى لاحقاً الوصول لهذه الخدمة عن طريق الاسم .
ZIP	**Zone Information Protocol**	البروتوكول المسؤول عن إدارة (**Zones**) او تفرعات الشبكة.
ATP	**AppleTalk Transaction Protocol**	البروتوكول المسؤول عن إرسال إشعار حول وصول الـ **Packets** الى وجهتها.
ATP	**AppleTalk Session Protocol**	برتوكول يقدم كافة الخدمات الضرورية للوصل الى **AppleShare server** .
ATP	**Printer Access Protocol**	البروتوكول المستخدم للوصول إلى الطابعات الموصلة بالشبكة.
ATP	**AppleTalk Filing Protocol**	البروتوكول المستخدم في مشاركة الملفات عبر الشبكة.
AEP	**Apple Talk Echo Protocol**	البروتوكول المستخدم لتحقق ما اذا كانت الأجهزة متصلة في الشبكة أم لا فهو يشبه عمل الـ **Ping** .





أيمن النعيمي - سوريا

اولى خطوات إحتراف عالم النسخ الاحتياطي

يعتبر عالم النسخ الأحتياطي أو الـ Backup هو أحد أهم وظائف أي مهندس شبكات مسؤول عن شبكة ما لذا قررت أن اقدم لكم مجموعة من المقالات التى تقدم صورة نظرية وعملية لكيفية بناء أفضل طريقة للنسخ الأحتياطي والتى سوف نبدأها بسؤال عن ماهية المعلومات التى يجب أن نقوم بعمل نسخ أحتياطية منها.

فالمعلومات وأهميتها حقيقة هو السؤال الأول والاهم فهو يحدد كل شيء خاص بعملية النسخ الأحتياطية ويحدد سياساتها فلو كانت المعلومات ليست بتلك الاهمية عندها لايوجد داعي ابدا لعملية الحفظ الأحتياطي لكن السؤال الصحيح الذي يجب أن نطرحه الآن على أعتبار أننا متفقين على أن المعلومات هامة ويجب أخذ نسخة منها هو ماهي المعلومات التى يجب أن أخذ نسخ أحتياطية منها ؟

هل حفظ معلومات الجهاز كله سوف يكون الحل الأنسب ؟

منطقيا نعم لكن عمليا أعتبره شيئ غير ذكي ولايعكس عقلية مهندس كمبيوتر حقيقي, لأن حجم المعلومات المحفوظة سوف يزيد يوما بعد يوم والوقت الذي سوف تستغرقه كل مرة لأرجاع نسخة أحتياطية إلى الجهاز كبيرا جدا مقارنة مع طرق آخرى بالاضافة إلى مستودعات التخزين التى سوف تكثر وسوف تصبح عبئ كبير عليك وعلى الشركة لعدة أسباب ومن أهمها خطورة وطريقة تأمينها بشكل جيد. لكن نستطيع أن نتفق أن كل ماتحدثت عنه يمكن تجاهله ببساطة لو في حال كان لديك عشرة أجهزة أو أثنا عشر جهاز فهنا الموضوع أبسط ويمكن عمل نسخ أحتياطية كاملة لكل الأجهزة لكن ماذا لو كنا نتحدث عن مئة جهاز أو ألف جهاز مثلا ؟

هل أحتاج إلى عمل نسخ أحتياطية من ملفات نظام التشغيل والبرامج الموجودة على كل جهاز على حدى ؟

تخيل معي أن لديك خمسين جهاز في الشركة وأنت تقوم بعمل نسخة كاملة لكل ماهو موجود على الهارد ديسك وهي ليست المشكلة الحقيقة لان المشكلة هي تكرار الملفات الموجودة مسبقا على الجهاز فلقد يكون هدفنا من أستعادة الملفات هو أستعادة ملف واحد حذف بالغلط والنتيجة سوف تكون أستعادة كل الملفات السابقة والذي قد يؤثر على عملنا وعلى عمل نظام التشغيل المثبت لو في حال لم يكن الحفظ بشكل يومي. والنتيجة التى أريد أيصالها لك من هذه الفقرة هي ضرورة تحديد وأرشفة ملفات المستخدم الموجودة على الجهاز فقط فهي الوحيدة التى تهمنا في عملية حفظ النسخ الاحتياطية من الاجهزة وباقي الملفات ليست بالمشكلة الكبيرة والحل الأمثل هو أن تكون ملفات المستخدمين تحفظ مباشرة على السيرفر أو الدومين لأن العمل عندها سوف يكون بسيط وسهل جدا عليك لأنك حينها لن تحتاج لعمل نسخ أحتياطية لكل جهاز على حدى يكفيك عمل نسخة أحتياطية لملفات السيرفر وأنتهى الأمر.

هل أحتاج إلى عمل نسخ أحتياطية لكل الملفات التى تخص المستخدم ؟

عادة يملك المسخدم بعض الملفات التى لاتحتاج إلى عمل نسخ أحتياطية منها مثل ملفات الموسيقى والصور الشخصية المفضلة والخ... وبالتالي سوف تحصل على نسخ أحتياطية لملفات هامة وغير هامة وهي النقطة الثانية التى يجب أن تضعها ضمن سياسات الـ Backup وهي تحديد ملف للمستخدمين ليضعوا فيه ملفاتهم وأشيائهم الشخصية تحت عنوان لاتقوم بحفظه او اي أسم أنت تختاره.

من ناحية آخرى عندما نتكلم عن الـ Backup يجب أن نميز بين الجهاز العادي الخاص بالمستخدمين وبين السيرفرات لان الوضع هنا يتغير تماما لأن السيرفر يحتاج حرص أكبر من الاجهزة العادية لأن وجود هذه الأجهزة ووجود ملفاتها يؤثر على العمل بشكل مطلق لذلك السيرفر يحتاج منك أخذ نسخة أحتياطية من كل الملفات الموجودة وهذا يشمل ملفات النظام والتعريفات وكل ماهو بداخله لأن توقف عمل هذه الأجهزة لساعة واحدة قد يكون له تأثير على الشركة وعلى مستقبلك في الشركة ويفضل دائما الأعتماد على نظام RAID مع الهارد دسك الخاص بالسيرفرات وأحب أن أشير إلى نقطة هامة وهي RAID لايعتبر نظام للنسخ الأحتياطية بل هو نظام يساعدك في تخفيض نسب خطورة حدوث مشكلة في الهارد دسك.

وآخيرا أعلم أن كل شيء نسبي وكل السياسات التى تحدثنا عنها متغيرة بحسب عدة عوامل تعتمد على حجم وأهمية وجوهر البيانات وطبعا مكان العمل فقد تحتاج أن تقوم بنسخ كل البيانات الموجودة على أحد الأجهزة لأن توقف أحد الأجهزة قد يسبب مشاكل كبيرة في العمل وهدف المقال الأول هو توضيح كل النقاط التى يجب أن تضعها نصب عيناك عندما يطلب منك عمل Backup للاجهزة ويفضل دائما أن تتناقش مع أصحاب العمل موضوع السياسات التى يجب أتباعها في عمل الـ Backup حتى لاتتحمل أي مسؤولية قد تسبب مشاكل لك مستقبلا في العمل

المنظمات المحلية لتنظيم العمل بالشبكات اللاسلكية
Regulatory Domain Governing Bodies

اذا كنت مصريا ستنزعج قطعا اذا قلت لك كم ميلا تقطعها سيارتك من بيتك الي العمل ستنزعج أكثر اذا طلبت منك أن تذكر لي وزنك بالرطل وربما ستضربني لو سألتك كم طولك بوحدة القدم العيب ليس فيك العيب فيمن سألك فهو لم يتوخي الدقة في استخدام الوحدات التي تستخدم في بلدك

ففي مصر نستخدم الكيلو متر للمسافات الطويلة و الكيلوجرام للأوزان والمتر للأطوال القصيرة و هي ايضا الوحدات الدولية التي تستخدم في الكثير من الدول

ففي حين لازالت بعض الدول تستخدم بعض الوحدات كالرطل و القدم و الميل كنوع من الهوية فهناك دول تستخدم وتعتمد الوحدات الدولية لمقاييسها ولعل من يدرس منكم الفقه يجد بعض أنواع من الوحدات التي لم تعد موجودة الا عند استخدامها شرعيا مثل المد والصاع و الفرسخ و مد البصر و القلة وهناك الرطل العراقي والرطل الشامي وغيره

و الأمر الذي ربما لا تعرفه ان الوحدة نفسها يختلف قياسها من مكان الي اخر علي سطح الكرة الأرضية وفي باطنها ايضا

ففي حين تبلغ كتلتي 60 كجم في مصر فقد اكون اثقل قليلا عند خط الإستواء و بالطبع لن أذهب اطلاقا الي أحد القطبين الشمالي والجنوبي لأني بصراحة لا أريد ان اكون أخف مما أنا عليه و سأسعد حقا اذا اقتربت اكثر من مركز الكرة الأرضية لأن كتلتي ربما ساعتها ستتخطي مائة كيلوجراما

هل هذه حقائق علمية ؟

نعم سيدي حقائق علمية فلابد أن تضعها في



اعتبارك عند تصنيع مكونات موجهة الي قطر معين

عندما كنا طلاب في قسم الإتصالات بكلية الهندسة الإلكترونية كنا نحب اقتناء الكتب الحديثة التي بها دارات الكترونية كي نقوم بتصنيعها وكم تكون مدي فرحتنا عندما تنجح هذه الدائرة في عملها خاصة دوائر التحكم الألي عن بعد و دوائر الإستقبال وا لإرسال اللاسلكي وكان دائما يسترعي نظرنا تحذير هام في اخر سطر

«تحذير هام : حاول ان تراجع اعداداتكم الفيدرالية بخصوص التقنيات اللاسلكية » طبعا الصيغة التحذيرية أمريكية بحته

ان الأمر ليس هينا فقد تقوم بصنع دائرة تلتقط صدفة ترددات عسكرية او ترددات أجهزة المخابرات او الشرطة او تتداخل مع ترددات محجوزة مسبقا ولعلكم تتابعون بعض الأفلام التي تتحدث عن هذا الأمر

اذن فالأمر مازال يتعلق بالدول وتراثها الداخلي وهويتها و أحيانا لموقعها الجغرافي و طبيعة

وجودها وقربها من مركز الأرض و ايضا لسياسات أخري لا مجال لذكرها
هذا بالضبط ما أريده ففي عالمنا اللاسلكي توجد منظمات اقليمية علي عاتقها تنظيم هذه الأشياء في نطاقات جغرافية محددة منهاFCC وETSI وTELEC



FCC
Federal Communications Commission
لجنة الإتصالات الفيدرالية

مؤسسة مستقلة موجوده في الولايات لمتحدة الأمريكية انشئت في 1934 و علي عاتقها كل ما يختص بتقنيات ومواصفات الإتصالات السلكية واللاسلكية مثل الراديو والتليفزيون والكابلات والأقمار الصناعية و حيث ان الواي فاي يستخدم موجات الراديو فهو يقع تحت هذه المنظمة ، تعتمد عليها كامل أمريكا الشمالية و أمريكا الوسطي و استراليا ونيوزيلاندا وبعض أقطار اسيا



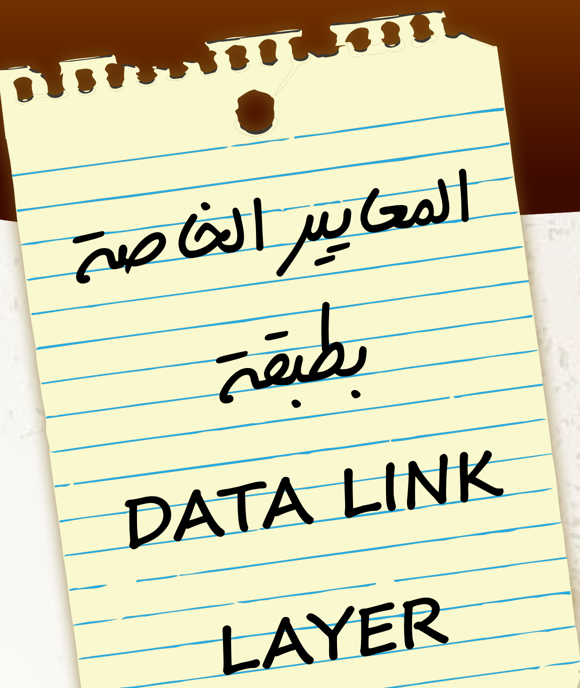
(ETSI)
European Telecommunications Standards Institute
المعهد الأوروبي للإتصالات

تم انشاؤها من قبل الأقطار الأوروبية تختلف عن سابقتها ان اعداداتها ليست الزامية علي الدول المختصة بها بل تعتبر كمنظمة استشارية تسترشد بها خارج القارة الأوروبية الشرق الأوسط و أفريقيا و بعض المناطق في اسيا



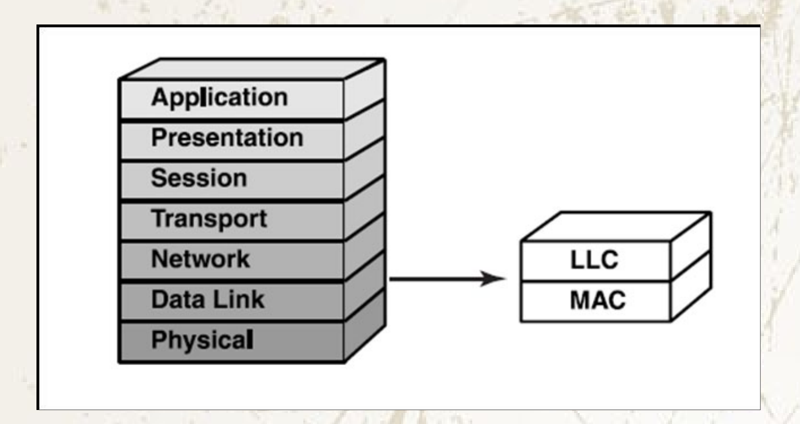
TELEC
the Telecom Engineering Center
مركز الإتصالات الهندسي

و هي ضمن وزارة الإتصالات والبريد اليابانية وهي تشبهFCC ولكنها في اليابان فقط
في النهاية اعلم أن لكل من هذه المنظمات عوامل و مقاييس مختلفة بالنسبة للهوائيات , و الإرسال والإستقبال و تقوم الأقطار الأخري خارج النطاق الجغرافي لهذه المنظمات بتتبع احدها واستخدام شروطها و مقاييسها ضمن اعداداتها المحلية و تكون الزامية لمواطنيها و الشركات العاملة بها



الكثير منا قد كتب حول مايسمى طبقات OSI التي تمثل طريقة انتقال المعلومة من جهاز لآخر , ومن أهم الأجهزة التي تعمل على الطبقة الثانية DATA LINK هو جهاز السويتش الذي يربط عدد كبير من الحواسيب في شبكة واحدة وضمن هذه الطبقة تم اعتماد معايير موحدة من أجل توحيد المنتجات الخاصة بهذه الطبقة لنتمكن من ربط الشبكات مع بعضها نظرا لوحدة المعايير التي تعمل عليها هذه الأجهزة , سوف نستعرض مبدئيا الأساسيات الخاصة بهذه الطبقة ومن ثم سنبحث فيما يسمى معايير 802 التي تبنى وفقها معظم المنتجات والاجهزة الخاصة بالطبقة الثانية DATA LINK

فمن المعروف أن DATA LINK LAYER تتألف من طبقتان فرعيتان هما MAC – LLC MEDIA ACCESS CONTROL و طبقة LOGICAL LINK CONTROL وهما مسؤولتان عن عدة مهام في عمل الشبكة ابتداءا عن العنوان الفيزيائي MAC ADDRESS بالاضافة الى مايسمى TOPOLOGY الخاص بالشبكة وهو تكوينها الفيزيائي والمنطقي وكذلك التحكم بطرق الوصول ACCESS CONTROL METHOD



العنوان الفيزيائي
MAC ADDRESS

العنوان الفيزيائي MAC ADDRESS والذي يكون فريدا لكل كرت شبكة في العالم ويتألف من عنوان يستخدم 12 خانة HEXADECIMAL بحجم 48 بت كالعنوان التالي :

07-57-AC-1F-B2-76

وجاءت تسميته من كونه يندرج ضمن الطبقة الفرعية المسماة MAC ويقسم هذا العنوان الى فرعين رئيسيين فأول ثلاثة خانات مزدوجة كما في مثالنا AC:07:57: تسمى organizationally unique identifier والتي تتحكم منظمة IEEE بها لضمان عدم تكرار هذا العنوان الفيزيائي في أكثر من كرت حول العالم في حين أن القسم الآخر من العنوان الفيزيائي والذي يتمثل بالثلاث خانات الأخرى فانها يتم اختيارها من خلال الشركة المصنعة وكذلك يجب أن تراعي عدم تكرار هذه الخانات بين منتجاتها وبتكامل هذين الجزئين يمكننا القول أن هذا العنوان الى حد كبير يكون فريدا حول العالم

عادة هذا العنوان لايمكن تغييره وتقوم الشركة عادة بتسجيل العناوين التي استعملتها لمنع تكرار استخدامها كما تشرف كما قلنا IEEE على ضمان ذلك ولكن يمكن لمدراء الشبكة باستخدام برمجيات الشركات المصنعة من تغيير هذا العنوان في حالة (وهي نادرة الحدوث جدا) كون الشبكة تتضمن عنوانين فيزيائيين متماثلين لاثنين من كروت الشبكة

NETWORK TOPOLOGY

تتم عملية تكوين مايسمى ب NETWORK TOPOLOGY من خلال طبقة DATA LINK LAYER ويمكن تعريف هذا المصطلح بأنه الطريقة التي تدرك فيها أجهزة الشبكة طريقة التعامل مع الشبكة وتكوينها وينقسم الى نوعين :

1 - فيزيائي وهو طريقة توضع الكابلات في الشبكة

2 - المنطقي والذي يعبر عن طريقة تدفق وانتقال البيانات

فمثلا هناك شبكات STARوهذا هو التصميم الفيزيائي للشبكة في حين أن تعبير شبكة ETHERNET هو تعبير يعبر عن البروتوكول وتقنية النقل المستخدمة في نقل البيانات والتي هي أحد انواع التصميمات المنطقية

Bus Ring Star
Extended Star Hierarchical Mesh

معيار 802.

كنتيجة لتطور الشبكات ورغبة من الشركات في الاتفاق على معايير معينة في التصنيع من أجل الوصول الى معايير لمنتجات تعمل مع بعضها مما يسهل التكامل بين الشبكات فلقد طورت منظمة INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERING معيار 802 وهو معيار يعمل ضمن طبقة DATA LINK ويتضمن هذا المعيار خصائص للشبكات المصنعة وفقا لهذه المعايير وهذه الخصائص هي السرعة وطرق الوصول والأجهزة المستخدمة بالاضافة الى التصاميم (TOPOLOGY)
ولقد جاءت تسمية هذا المعيار من العام الذي تم الاجتماع به وهو 1980 بنما رقم 2 فانما يشير الى الشهر الثاني من ذلك العام وهو الشهر الذي تم فيه الاجتماع وتشير بعض المعايير المبنية على هذا المعيار الى نوع معين من التصميم التكنولوجي بينما نجد أن بعض المعايير الأخرى مثل المعيار 802.3 الى نظام شبكي متكامل من حيث التصميم المنطقي والفيزيائي وطرق الوصول المستخدمة
وسنتناول الآن أهم التقنيات المبنية على المعيار 802.

802.1 LAN/MAN BRIDGING -MANAGEMENT

ويعرف هذا المعيار أنظمة ادارة الشبكات ومعايير الاتصال مابين الأجهزة ويضع مواصفات لعمل بعض التقنيات المستعملة في الراوترات والسويتشات ومن أهم التقنيات المشتقة من هذا المعيار هي تقنية SPANNING TREE ALGORITHM والتي تستعمل في السويتشات لمنع حدوث مايسمى NETWORK LOOP ضمن الشبكة

802.2 LLC SUBLAYER

هذا المعيار خاص بالطبقة الفرعية المسماة LLC ضمن طبقة DATA LINK وتشكل واجهة للتواصل مابين الطبقة الفرعية MEDIA ACCESS CONTROL ومابين NETWORK LAYER

802.3 CSMA/CD

وهو خاص بالشبكات التي تستعمل BUS كتصميم باستخدام تقنية BASEBAND مع ملاحظة استعمال طريقة وصول تسمى Carrier Sense/Multiple Access (with Collision Detection (CSMA/CD ويستعمل هذا المعيار بكثرة ويعرف باسم ETHERNET وهناك اصدارات حالية من هذه التقنية تدعم سرعات حتى 1 غيغا بت / ثانية



802.5 TOKEN RING

وهو المعيار الخاص بالمنتجات التي تعرف بشبكات TOKEN RING مع هذا المعيار من الممكن استخدام انواع مختلفة من الكابلات مثل TWISTED PAIR ومن الممكن أن تعمل بسرعة 4 الى 16 ميغا بت في الثانية وتعمل مع تصميمات مختلفة مثلPHYSICAL STAR LOGICAL RING – باستخدام تقنية وصول تسمى TOKEN PASS وهي أحد التقنيات التي لاتزال مدعومة من قبل شركة IBM .
ومن المميزات المهمة لهذه التقنية أنها تقوم باعادة بث البيانات عند مرورها بكل جهاز تفاديا لضعف الاشارة مما يجعل الأجهزة المبنية على هذا المعيار أكثر كلفة مقارنة بتقنية كالـ ETHERNET مثلا

802.10 LAN MAN SECURITY

وهو معيار مصمم لتأمين الشبكات في بيئة – LAN MAN يعمل هذا المعيار عن طريق الاندماج في حزم البيانات الخاصة ب FRAME لتأمين الحماية في بيئة الشبكات الافتراضية VLAN حيث يمنع التبادل مابين الحزم الخاصة بأحد الشبكات الافتراضية وبين غيرها من الشبكات الغير محمية ويؤمن هذا المعيار الوثوقية والتشفير المطلوبين لضمان أمان المعلومات ولقد لقي رواجا كبيرا في الفترة الأخيرة خصوصا بعد اعتماده ضمن بروتوكول IEEE 802.1Q الخاص بأجهزة سيسكو



802.11 WIRELESS LAN

من أهم المعايير المبنية على هذا المعيار 802.11 A-B-G-N وهذه المعايير تطورت سرعات النقل فيها من 11 ميغا بت في المعيار 802.11 B ليصل الى 54 ميغا بت في المعيار 802.11 G وليصل الى 300 ميغا بت في بعض الاصدارات من معيار 802.11 N ومعظم هذه المعايير تستخدم ترددات من فئة 2.4GHZ في حين ان معيار 802.11A يستخدم تردد 5 GHZ مما يجعل الأجهزة المبنية وفقا له غير متوافقة للعمل مع الاصدارات الأخرى

802.12 DEMAND PRIORITY ACCESS METHOD

وطور هذا المعيار بداية من قبل شركة HP وهو يجمع المعيارين ETHERNET & TOKEN RING ويعتمد على منهجية تسمى DEMAND PRIORITY ويستخدم عادة أجهزة شبكة ذكية حيث يميز بين الFRAME استنادا الى الافضلية الممنوحة لها حيث يقوم جهاز الشبكة بالبحث بين المنافذ عن المنفذ الذي يحمل FRAME ذات أفضلية عالية من خلال حجم البيانات المتدفقة منه ويعتبر مثالي للشبكات التي تستخدم لنقل بيانات الصوت والفيديو مباشرة.

الاجهزة المستخدمة في طبقة DATA LINK

هناك ثلاثة أجهزة رئيسية تستخدم فيهذه الطبقة وهي

BRIDGE

وهو جهاز يعمل على طبقة DATA LINK يقوم بتقسيم الشبكة الى قسمين بحيث تبقى بالنسبة لطبقات الشبكة العليا شبكة واحدة والغاية من هذا التقسيم هو التخفيف من الازدحام على الشبكة وبتقسيم الشبكة الى جزئين لن تعبر البيانات من قسم الى أخر الا اذا كانت تابعة لهذا القسم وكل ماعدا ذلك تبقى في نفس القسم مما يحسن من أداء الشبكة ويخفف الازدحام بشكل ملحوظ

SWITCH

وهو الجهاز الذي يعتبر أكثر ذكاء من HUB لأنه لايقوم بالربط بين أجهزة الشبكة ونشر كل الحزم الواردة من المنافذ الى كل المنافذ كما يفعل HUB حيث يتسبب ذلك بازدحام وبطء في الأداء اما السويتش فيقوم بانشاء جدول بعناوين MAC الخاصة بالأجهزة المرتبطة به مما يجعله يوجه الحزم المرسلة من أحد الأنظمة وفقا لعنوان الMAC الموجود فيHEADER ولايقوم بنشرها على كل المنافذ مما يخفف من الازدحام ويعطي أداء أفضل وأكثر تنظيما

WAP"WIRELESS ACCESS POINT "

وهو الجهاز الذي يستخدم للربط بين الشبكة السلكية واللاسلكية ويقوم بنشر الحزم الواردة الى كل الأجهزة المتصلة السلكية واللاسلكية ويزود عادة بأنتينا ويم ّكن المستخدمين المتصلين عبر الشبكة السلكية من الاتصال بالأجهزة المتصلة بالشبكة اللاسلكية

يمكنك تصفية المتصلين بالشبكة وفقا لما يسمى MAC FILTERING والذي يسمح بالعبور أو لايسمح للمستخدمين الذين ترد عناوينهم الفيزيائية ضمن القائمة قائمة التصفية كونه يعمل على طبقةDATA LINK ويتمكن من التحكم بالحزم والأجهزة المتصلة وفقا لعناوينها الفيزيائية





عادل الحميدي

الموجه Router
& التوجيه Routing

من منا لم يسمع بالروتر أو لم يتعامل معه، فأغلبنا وإن لم يكن جميعنا تعامل معه وقام بتجهيزه فهو عصب الشبكة وهو العقل المفكر فيها، لذلك قررت تخصيص مقالة هذا الشهر عن العقل المفكر والمدبر للشبكة بحيث نتناول آلية عمل هذا الجهاز بالإضافة إلى بعض البروتوكولات التي تدعم عمله.

ولو سأل مبتدأ ما هي وظيفة الروتر Router كجهاز داخل الشبكة؟ وكيف يقوم بهذه الوظيفة؟ فسأقول له تابع معنا لكي تتعرف على الإجابات التفصيلية لهذه الأسئلة

جداول التوجيه والشبكات المتصلة مباشرة Routing Tables And Networks Directly Connected

تعتبر وظيفة الروتر الأساسية توجيه حزم البيانات Packets للوجهة المطلوبة، وحتى يقوم الروتر بعمليه توجيه حزم البيانات تلك من شبكة لأخرى، يجب أن يحتوي ضمن ذاكرته على جدول يسمى جدول التوجيه Routing Table، يحتوي هذا الجدول بداخله على جميع الشبكات الرئيسية والفرعية، ليس هذا فحسب بل وطريقة الوصول لكل شبكة من تلك الشبكات.

لكي يستطيع الروتر توجيه البيانات إلى أي جهاز بالشبكة يجب أن يحتوي في جداوله جميع أرقام الشبكات الموجودة، وبالتالي إذا كان لدينا خمس شبكات فرعيه فإنه حتى تستطيع الروترات توجيه حزم البيانات لأي وجهة كانت؛ يجب أن يحتوي كل روتر في جدوله على تلك الخمس شبكات، عندما نقوم بتشغيل الروتر لأول مرة وقبل البدء بإعطاء عناوين IP للمنافذ يكون جدول التوجيه فارغاً ولا يستطيع الروتر التعرف ولا حتى على أرقام الشبكات المتصلة به مباشرة، لكن بعد إعطاء المنافذ عناوين IP سيقوم الروتر بإضافة مسارات للشبكات الموصولة به بشكل مباشر عن طريق تلك المنافذ، وهذا أول ما يكتب في جداول التوجيه بشكل أوتوماتيكي ولا يحتاج لتدخل منا.

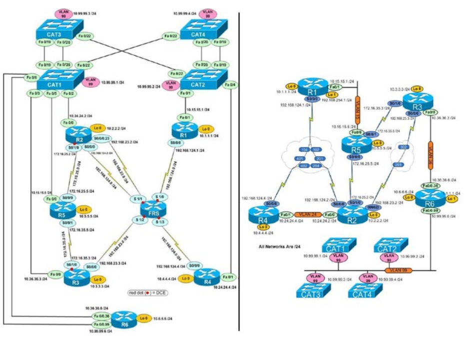
نستنتج مما سبق أنه من المعلومات المهمة التي يعتمد عليها الروتر ليؤدي وظيفته هي جداول التوجيه، فمن خلال هذه الجداول يصنع الروتر قراراته في توجيه البيانات.

ولكن كيف يتم بناء جداول التوجيه؟

التوجيه الساكن:

التوجيه باستخدام المسارات الساكنة Static Routing

يقوم الروتر بإضافة أرقام الشبكات المتصلة به مباشرة فور إعداد عناوين IP وتفعيل المنافذ، ولكن نلاحظ أن الروتر بهذه المرحلة يستطيع الاتصال فقط مع هذه الشبكات، أما الشبكات الأخرى الموصولة على الروترات الأخرى فلا يستطيع أن يصل إليها.



إذن كيف يتعرف الروتر على هذه الشبكات؟ أو بعبارة أخرى كيف يبني الروتر بقية جدول التوجيه الذي يحتوي على الشبكات الغير متصلة به بشكل مباشر؟

يتم بناء جداول التوجيه إما يدوياً static (من قبل مسئول الشبكة) أو بصفة أوتوماتيكية dynamic (من خلال بروتوكول من بروتوكولات التوجيه)، فعملية إنشاء جداول التوجيه يدوياً ممكنة على الشبكات الصغيرة أو في بعض الحالات الخاصة وهذا ما يدعى التوجيه الساكن Static Routing، لكن على الشبكات الكبيرة تعتبر هذه العملية شاقة جداً وفي بعض الحالات تكون غير ممكنة، لذا تتم عملية إنشاء الجداول بصفة أوتوماتيكية في الشبكات الكبيرة ومن خلال بروتوكولات مختصة، تستخدمها الروترات لتبادل المعلومات عن نفسها وعن الشبكات المحيطة بها.

من بين هذه البروتوكولات نذكر: RIP, EIGRP, OSPF

ملاحظة: جدول التوجيه هو عبارة عن قائمة تحتوي على عناوين الشبكات وعناوين الروترات التي يستطيع النظام استخدامها للوصول إلى تلك الشبكات (تعريف مبسط).

التوجيه الديناميكي:

أساسيات التوجيه الديناميكي Dynamic Routing Fundamentals

تقوم الروترات بتوجيه حزم البيانات ديناميكياً باستخدام بروتوكولات التوجيه وذلك من خلال قيام بروتوكولات التوجيه الموجودة بكل روتر على الشبكة ببناء جدول التوجيه ثم تحديثه بشكل مستمر بحيث يكون لدى كل روتر جدول يحتوي على مسارات لجميع الشبكات المتاحة.

إذا استقبل بروتوكول التوجيه في روتر ما مسارين لنفس الشبكة من مصدرين مختلفين فإن الروتر يضع في جدول التوجيه المسار ذو المقياس الأقل Lowest Metric، بمعنى أنه وباستخدام مقياس Metric معين وخاص به (يختلف المقياس من بروتوكول لآخر) يحدد المسار الأفضل.

عندما يصبح أحد المسارات المؤدية لشبكة ما غير متاح بسبب مشكلة ما، فإن البروتوكول يحذف هذا المسار من جدول التوجيه، ثم يقوم البروتوكول بالبحث عن مسار بديل يؤدي لهذه الشبكة.

ملاحظة: يسمى الزمن الفاصل بين اكتشاف الروتر للمسار غير المستخدم وبين استبداله بمسار آخر بزمن التقارب Convergence Time.

ملاحظات وتعريفات هامة:

الخوارزمية: هي حل تفصيلي لمشكلة ما.
تحديد المنفذ الذي يجب إرسال الحزمة Packet الواردة إليه بجهاز التوجيه هي مهمة بروتوكولات التوجيه حيث تستخدم لذلك خوارزميات توجيه مختلفة وهذه الخوارزميات تعتمد على مقاييس التوجيه Metric. بمعنى آخر الخوارزمية هي تلك الخطوات التي يسير عليها بروتوكول التوجيه لبناء جدول التوجيه وحل مشاكله، وأحد أهم تلك الخطوات هي المقياس الذي يحدد من خلاله أفضل مسار لوجهة معينة ليضعه في جدول التوجيه.

نوع التحديث:

يقصد بنوع التحديث: جداول التوجيه التي تتبادلها الروترات مع بعضها البعض، والتحديث يتم بإحدى الطريقتين:

- Full Updates: يقوم البروتوكول بإرسال جدول التوجيه كاملاً إلى الروترات الأخرى.
- Partial Updates: يقوم الروتر بإرسال جزء من جدول التوجيه يتضمن فقط المسارات التي تم تغييرها.

نوع الإرسال:

عندما يقوم الروتر بإرسال معلومات جدول توجيهه إلى الروترات الأخرى، والإرسال يتم بإحدى الطريقتين:

- Broadcast: تصل التحديثات لجميع روترات الشبكة حتى التي يعمل عليها بروتوكول مختلف عن البروتوكول الذي أرسل التحديثات.
- Multicast : تصل التحديثات فقط للروترات التي تحوي نفس بروتوكول التوجيه الذي أرسل التحديثات.

زمن التقارب:

يقصد فيه الزمن الفاصل بين اكتشاف البروتوكول لوجود خلل في أحد المسارات بجدول التوجيه وبين استبداله بمسار آخر، والبروتوكولات صنفين من حيث زمن التقارب:

- Fast Convergence: يقوم البروتوكول بالاستبدال بسرعة خلال ثواني.
- Slow Convergence: يقوم البروتوكول بالاستبدال ببطء، قد يصل الزمن لعدة دقائق.

المقياس:

يعبر عن قيمة عددية ترتبط بكل مسار يؤدي إلى شبكة ما، وتكون هذه القيمة معبرة عن أفضلية المسار بالنسبة للمسارات الأخرى المؤدية إلى نفس الشبكة، وتختلف هذه القيمة من بروتوكول لآخر ولكن جميع البروتوكولات تتفق بأن المسار ذو القيمة الأقل لقيمة Metric يكون الأفضل دائماً.

دعم طول القناع المتغير:

عند عنونة الشبكات بعناوين IP وتحديد القناع Mask لكل شبكة من هذه الشبكات فإنه من الممكن استخدام قناع موحد ومتشابه لكل الشبكات أو استخدام أطوال مختلفة، تسمى الشبكات التي تستخدم قناع شبكة متغير بالشبكات (Variable Length Subnet Mask (VLSM، أما الشبكات التي تستخدم أطوال ثابتة فتسمى(Fixed Length Subnet Mask (FLSM، لذلك نستطيع تصنيف البروتوكولات الداخلية صنفين:

- Classless: تستخدم في شبكات VLSM.
- Classfull: تستخدم في شبكات FLSM.

مصدر البروتوكول:

ويقصد بذلك المنظمة التي طورت البروتوكول وهنا لدينا نوعين من البروتوكولات:

Cisco Proprietary: من إنتاج وتطوير Cisco، ويعمل فقط على روترات Cisco.

Standard: قياسي يعمل على روترات جميع المزودين.

أكثر المقاييس شيوعاً مع بروتوكولات التوجيه: Metric

1 - Bandwidth: عرض النطاق الترددي، مثال/ يفضل ارتباط Ethernet ذو السرعة 100 ميجابت/ ثانية على خط سرعته 64 كيلوبت/ ثانية.

2 - Delay: فترة التأخر هي المدة الزمنية المطلوبة لنقل حزمة عبر كل ارتباط من المرسل (المصدر) إلى المستقبل (الوجهة)، وهي تعتمد على: عرض النطاق - مقدار البيانات التي يمكن تخزينها مؤقتاً بجهاز الروتر - ازدحام الشبكة - المسافة المادية.

3 - Load: الحمل وهو مقدار النشاط على مورد شبكة روتر مثلاً أو ارتباط.

4 - Reliability: وثوقية الارتباط وهي معدل الأخطاء لكل ارتباط في بنية الشبكة.

5 - Hop Count: تعداد الخطوات حيث تفضل المسار ذو أقل عدد من أجهزة الروترات.

6 - Cost: التكلفة وهي قيمة عشوائية تستند في العادة إلى: عرض النطاق الترددي - التكاليف المادية - قياسات أخرى بواسطة مسؤول الشبكة.

ولكن أين يتم حفظ جدول التوجيه في الروتر؟

يتم حفظ جدول التوجيه في الروتر بالذاكرة RAM والتي تكون فارغة عندما يبدأ الروتر بالتشغيل.

ملحوظة هامة: يحتوي الروتر على عدة أنواع من الـ Memories الذواكر منها Random Access Memory(RAM) ذاكرة الوصول العشوائي وهي تفقد محتوياتها عند انقطاع التيار الكهربائي عن الروتر أو عند إعادة تشغيله، ومنها Non-Volatile Random Access Memory (NVRAM) ذاكرة الوصول العشوائي غير المتطايرة وهي تحتفظ بالمعلومات حتى بحالة انقطاع التيار الكهربائي.
وقد يتساءل البعض لماذا لا يحتفظ الروتر بجدول التوجيه بالذاكرة NVRAM؟
والإجابة هنا بسيطة لا تحتاج إلى عناء وتفكير:
حيث الاحتفاظ بجدول التوجيه حتى بعد انقطاع التيارغير مناسب لأنه ربما فصلنا الروتر بغرض نقله ليعمل في مكان آخر، وبالتالي احتفاظه بجدول التوجيه يؤدي إلى خطأ جسيم، ففي كل مرة يبدأ الروتر فيها العمل عليه أن يقوم بجمع المعلومات عن الشبكة التي هو بها وبناء جدول التوجيه الحالي.

والآن أعرف أنك متشوق كثيراً لرؤية جدول التوجيه هذا الذي تحدثنا عنه خلال هذا المقال، ولكن كيف؟ وهل تريد أن تراه حقاً؟ لعرض جدول التوجيه Routing table بأجهزة الروترات الخاصة بسيسكو نستخدم الأمر:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
```

وهذه بعض الرموز التي ستظهر لك في نتيجة أمر العرض هذا:
C-connected: شبكة متصلة بالروتر مباشرة (يتعرف عليها تلقائياً كما ذكرنا)
S-static: شبكة متصلة بالروتر بشكل غير مباشر وعرفه عليها مسئول الشبكة (التوجيه الساكن)
R-RIP, B-BGP, D-EIGRP, O-OSPF, I-IS-IS: شبكة متصلة بالروتر بشكل غير مباشر وعرفها عن طريق أحد تلك البروتوكولات (التوجيه الديناميكي)
وإليك المثال التالي لجدول توجيه يحتوي على شبكات متصلة به بشكل مباشر وهي 1.1.1.1/32 و 192.168.1.0/24 و 192.168.2.0/30
وشبكات غير متصلة به بشكل مباشر وتعرف عليها من خلال البروتوكول OSPF وهي 2.2.2.2/32 و 3.3.3.3/32 و 192.168.3.0/24 و 192.168.4.0/30 و 192.168.5.0/24

```
Gateway of last resort is not set
is subnetted, 1 subnets 32/1.0.0.0
C       1.1.1.1 is directly connected, Loopback0
is subnetted, 1 subnets 32/2.0.0.0
0/via 192.168.2.2, 00:00:34, Serial1 [65/O       2.2.2.2 [110
is subnetted, 1 subnets 32/3.0.0.0
0/via 192.168.2.2, 00:00:34, Serial1 [129/O       3.3.3.3 [110
is subnetted, 1 subnets 30/192.168.4.0
0/via 192.168.2.2, 00:00:34, Serial1 [128/O       192.168.4.0 [110
0/via 192.168.2.2, 00:00:34, Serial1 [129/110] 24/O    192.168.5.0
0/is directly connected, FastEthernet0 24/C    192.168.1.0
is subnetted, 1 subnets 30/192.168.2.0
0/C       192.168.2.0 is directly connected, Serial1
0/via 192.168.2.2, 00:00:36, Serial1 [65/110] 24/O    192.168.3.0
```

بروتوكولات التوجيه الديناميكي:

ملحوظة: تعريف النظام المستقل Autonomous System (AS): هو شبكة أو مجموعة من الشبكات تخضع لتحكم إداري مشترك أو بمعنى آخر حيث يتكون من أجهزة روترات تمثل طريقة عرض متناسقة للتوجيه إلى العالم الخارجي، ويكون لكل نظام مستقل AS رقم خاص به AS Number.

تنقسم إلى:

أنواع بروتوكولات التوجيه Routing Protocol types

1) - عائلة بروتوكولات توجيه العبارة الداخلية Interior Gateway Routing Protocol: IGP

تقوم بتوجيه البيانات ضمن نظام مستقل، كما تقوم بتبادل معلومات التوجيه مع الروترات الموجودة بنفس النظام المستقل Autonomous System، مثال: RIP - IGRP - EIGRP - OSPF - IS-IS

وهي تنقسم إلى:

- بروتوكول متجه المسافات Distance Vector Protocol: ووظيفته يحدد كلاً من المسافة والاتجاه والمتجه إلى أي ارتباط (شبكة) في بنية الشبكة ويسجل ذلك في جدول التوجيه داخل الروتر. وهو لا يستهلك من موارد الروتر من معالج وذاكر الشيء الكثير، وهو سهل الإعداد والتشغيل على الروتر، ولكنه غير سريع. مثال: RIP - IGRP
- بروتوكول حالة الارتباط Link State Protocol: ووظيفته أنه صمم ليقوم بإنشاء الهيكل الكامل لبنية الشبكة كاملة في عدة جداول داخل الروتر ومنها يستنتج جدول التوجيه. لذلك فهو يستهلك موارد الروتر من معالج وذاكرة بشكل كبير فيحتاج لروتر ذو إمكانيات عالية، ويكون غير سهل عند الإعداد نوعاً ما، ولكنه نتيجة بناءه لهذه الجداول يكون سريع جداً عن النوع الأول. مثال: OSPF - IS-IS
- هجين/خليط Hybrid: (ويسمى أحيانا Advanced Distance Vector Protocol) وسمي بذلك لأنه يجمع بين خصائص متجه المسافات وحالة الارتباط. مثال: EIGRP

2) - عائلة بروتوكولات توجيه العبارة الخارجية Exterior Gateway Routing Protocol: EGP



تقوم بتوجيه البيانات بين الأنظمة المستقلة (AS) ، كما تقوم بتبادل معلومات التوجيه مع الروترات الموجودة خارج النظام المستقل Autonomous System، مثال: BGP

ملاحظة: سنقوم بهذا المقال بدراسة البروتوكولات الداخلية فقط، أما عن الخارجية فمثالها الوحيد هو البروتوكول BGP.

نبذة مختصرة جداً عن بروتوكولات التوجيه:

1 - بروتوكول معلومات التوجيه RIP:

هو بروتوكول توجيه متجه المسافات، يستخدم تعداد الخطوات Hop Count (عدد الروترات) كمقياس Metric لتحديد الاتجاه و المسافة إلى أي ارتباط في بنية الشبكة، فإذا كانت هناك عدة مسارات إلى وجهة ما فالمسار الأفضل هو ذو أقل عدد من الخطوات وهذا هو المقياس الوحيد الذي يستخدمه RIP، لذا فإنه لا يحدد دائماً أسرع مسار للوجهة النهائية، كما أن RIP لا يمكنه توجيه حزمة Packet لمسافة تتعدى 15 خطوة.

RIPv1: يتطلب قيام جميع الأجهزة المتصلة بالشبكة باستخدام نفس قناع الشبكة الفرعية نظراً لأنه لا يتضمن معلومات قناع الشبكة الفرعية Subnet Mask في تحديثات التوجيه.

RIPv2: يقوم بإرسال معلومات قناع الشبكة الفرعية Subnet Mask في تحديثات التوجيه، حيث يمكن أن تحتوي بنية الشبكة على شبكات فرعية مختلفة في قناع الشبكة الفرعية VLSM.

2 - بروتوكول توجيه العبّارة الداخلية IGRP:

هو بروتوكول توجيه متجه المسافات، قامت شركة سيسكو Cisco بتطويره خصيصاً لمعالجة المشكلات المرتبطة بالتوجيه في الشبكات الكبيرة التي فاقت نطاق بروتوكول RIP، وبإمكان IGRP تحديد أسرع مسار متاح بناءاً على: فترة التأخير Delay/ وعرض النطاق الترددي Bandwidth/ والحمل Load/ والوثوقية بالمسار Reliability/ وأقصى وحدة نقل MTU (Maximum Transfer Unit)، ويمكن لهذا البروتوكول أن يوجه حزمة لعدد أقصى من الخطوات يفوق RIP، ويستخدم التوجيه ذو الفئات FLSM فقط.

3 - بروتوكول IGRP المحسن EIGRP:

من البروتوكولات الخاصة بشركة سيسكو، وهو يوفر كفاءة التشغيل



فائقة مثل / التقارب السريع Very Fast Convergence وعبء منخفض على عرض النطاق الترددي، وهو بروتوكول متجه المسافات متقدم حيث يستخدم أيضاً بعض وظائف بروتوكول حالة الارتباط (فهو بروتوكول توجيه مختلط).

4 - بروتوكول فتح أقصر مسار أولاً OSPF:

هو بروتوكول توجيه حالة ارتباط تم تطويره بواسطة مجموعة عمل هندسة الإنترنت IETF عام 1988م، وقد تمت كتابته لتلبية حاجات الشبكات البينية الكبيرة المرنة التي لم يتمكن RIP من تلبيتها.

5 - بروتوكول نظام وسيط إلى نظام وسيط IS-IS:

هو بروتوكول توجيه حالة ارتباط يُستخدم مع البروتوكولات الموجهة بخلاف IP.

6 - بروتوكول عبّارة الحدود BGP:

وهو المثال الوحيد على بروتوكول العبّارة الخارجية EGP حيث يقوم بتبادل معلومات التوجيه بين الأنظمة المستقلة مع ضمان تحديد المسار دون حدوث حلقات loop، فهو بروتوكول إعلان المسار الأساسي المستخدم بواسطة موفري الخدمة SP (موفري خدمة الإنترنت ISP) على الإنترنت.

BGPv4: هو أول إصدار من BGP يدعم التوجيه المتبادل بين المجالات ويستخدم في ذلك التنظيم الهرمي للمسارات، ولا يستخدم المقاييس السابقة، بل يتخذ قرارات التوجيه استناداً إلى نُهج أو قواعد الشبكة باستخدام سمات مسار BGP المتنوعة BGP Attribute.

وهنا لابد مطرح سؤال مهم وهو ما هي الصفات التي يتصف بها بروتوكول التوجيه والتي تجعلنا نفضله على غيره؟ حيث ستعرف أن من أشهر البروتوكولات استخداماً في داخل النظام المستقل هو OSPF وخارجه لا يوجد غير BGP...

مواصفات خوارزميات البروتوكولات:

نهدف عند تصميم بروتوكولات التوجيه أن نجعلها تتصف بكل أو معظم تلك الصفات أو المواصفات...

لاحظ أن هذه الصفات والتدقيق فيها من الأهمية بمكان وقليلاً ما يتكلم عنها وقد تكون أدق ما في المقال لهذا الشهر: (لأنها ستساعدك في اختيار أنسب بروتوكولات التوجيه لتجعلها تعمل على روترات شركتك)...

1 - تحقيق الأداء الأمثل: يصف قدرة خوارزمية التوجيه على تحديد أفضل مسار بدقة، مثال/ EIGRP أدق من RIP حيث أن الـ EIGRP يستخدم أكثر من مقياس ليحدد المسار المفضل بشكل أدق ولا يحتمل الخطأ.

2 - البساطة والعبء المنخفض: كلما كانت الخوارزمية أبسط زادت كفاءة معالجتها بواسطة CPU المعالج وذاكرة الروتر، مثال/ أحياناً نضطر للتغاضي عن تلك الصفة لما نحصل عليه في النهاية من نتيجة أدق في الحسابات ورد فعل أسرع عند الأزمات والمشاكل كأن نفقد مسار فنوجد له بديل بشكل سريع Fast Convergence لذلك فإننا نفضل مثلاً OSPF على RIP.

3 - القوة والاستقرار: وهو أن تؤدي الخوارزمية عملها بشكل صحيح عندما تواجه ظروف غير معتادة أو غير متوقعة، مثال/ فشل الأجهزة - حالات زيادة الحِمل - أخطاء التنفيذ.

4 - المرونة: تكيف الخوارزمية بشكل سريع مع مجموعة متنوعة من تغيرات الشبكة، مثال/ توفر روتر جديد - ذاكرة الروتر - تغير عرض النطاق - تغير فترة تأخير الشبكة.

5 - التقارب السريع: هو عملية تعرف جهاز الروتر على المسارات المتاحة ببنية الشبكة لكل الوجهات أو بمعنى آخر هو عملية إيجاد مسار بديل لمسار فقد بسرعة، فالتقارب البطيء يجعل البيانات غير قابلة للتسليم، مثال/ OSPF يتقارب بسرعة، EIGRP يتقارب بسرعة جداً.

الخلاصة... هذا الجدول يأتي منه 30٪ من اختبار CCNA:

البروتوكول / وجه المقارنة	OSPF	EIGRP	IGRP	RIPv2	RIPv1
مصدر البروتوكول	قياسي Standard	Cisco	Cisco	قياسي Standard	قياسي Standard
النوع (بروتوكول العبّارة الداخلية IGP)	حالة الارتباط Link State	هجين/خليط Hybrid	متجه المسافات Distance Vector	متجه المسافات Distance Vector	متجه المسافات Distance Vector
المسافة الإدارية AD	110	90	100	120	120
نوع وطريقة الإرسال	Multicast	Multicast	Broadcast	Multicast	Broadcast
زمن كل إرسالية	كل 30 دقيقة أو إذا حدث تغير في الشبكة	إذا حدث تغير في الشبكة	كل 90 ثانية	كل 30 ثانية	كل 30 ثانية
العنوان المستخدم	224.0.0.5 & 224.0.0.6	224.0.0.10	255.255.255.255	224.0.0.9	255.255.255.255
نوع التحديث	Partial Updates	Partial Updates	Full Updates	Full Updates	Full Updates
طول القناع	VLSM Classless	VLSM Classless	FLSM Class Full	VLSM Classless	FLSM Class Full
زمن التقارب Convergence	Fast 10 sec	Very Fast 2-5 sec	Slow 3-5 min	Slow 3-5 min	Slow 3-5 min
المقياس المستخدم لتحديد أفضل مسار Metric	Cost (Bandwidth)	Bandwidth Delay Load Reliability MTU	Bandwidth Delay Load Reliability MTU	Hop Count	Hop Count
ملاحظات المقياس	—	يفضل: Bandwidth Delay	يفضل: Bandwidth Delay	Metric <= 15 Hop (Router) Metric > 15 Hop (Infinite)	Metric <= 15 Hop (Router) Metric > 15 Hop (Infinite)
الخوارزمية المستخدمة	Shortest Path First Algorithm (Dijkstra)	Diffusing Update Algorithm	Bellman-Ford Algorithm	Bellman-Ford Algorithm	Bellman-Ford Algorithm

ملحوظة: إذا وجدت أي إشكالات في الرموز أو الاختصارات بجدول المقارنة فارجع للمقالة ستجد فيها ما فاتك وأنك قرأتها على عجلة.

شهادة شكر وتقدير

تتقدم إدارة موقع



First Arabic Magazine for Networks

بالشكر والتقدير للمهندس العراقي

فادي الطه

لمشاركته الفعالة وجهوده المستمرة في إثراء الموسوعة العربية الخاصة بالشبكات
ومساهمته في الرقي بالمحتوى العربي التقني على الأنترنت

مؤسس ومدير موقع NetworkSet
المهندس أيمن النعيمي

2011 / 6 / 25